МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"

INFOSEC & COMPTECH

м. Кіровоград, 24-25 березня 2016 року

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

КІРОВОГРАДСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МЕХАНІКО-ТЕХНОЛОГІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА ПРОГРАМУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"

INFOSEC & COMPTECH

24-25 березня 2016 року

м. Кіровоград

УДК 004
Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей Міжнародної науково-практичної конференції, 24-25 березня 2016 року, м. Кіровоград: КНТУ, 2016. – 159 с.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Адреса редакційної колегії: 25030, м. Кіровоград, пр. Університетський, 8, Кіровоградський національний технічний університет, тел.: (0522)390-449.

Відповідальна за випуск: Мелешко Є.В.

Збірник містить тези доповідей за матеріалами Міжнародної науково-практичної конференції “Інформаційна безпека та комп'ютерні технології”, що відбулась 24-25 березня 2016 року на базі кафедри програмування та захисту інформації Кіровоградського національного технічного університету.

Матеріали збірника публікуються в авторській редакції. Відповідальність за зміст несуть автори.

ЗМІСТ

Секція 1.

Інформаційна безпека держави, суспільства та особистості

Секція 2.

Програмування та інформаційно-коммунікаційні технології

Секція 3.

Інтелектуальні системи та штучний інтелект

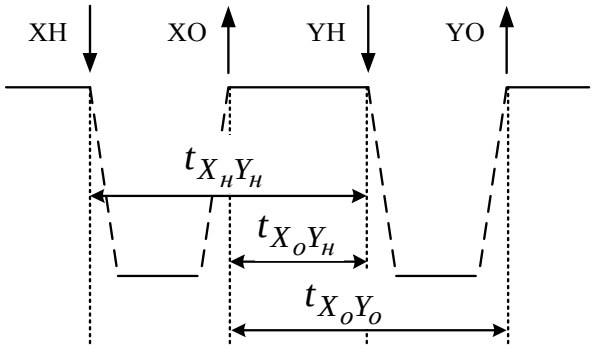
Секція 1.
Інформаційна безпека держави, суспільства та особистості

УДК 621.396:534

Алгоритм биометрической аутентификации на основе модифицированного метода диграфов

Алексеев В.А., аспирант, vasiliyalekseev.kh@gmail.com
Научный руководитель – Горелов Д.Ю., к.т.н., доцент
Харьковский национальный университет радиоэлектроники, г. Харьков

Одним из методов биометрической аутентификации пользователей по их клавиатурному почерку (КП) является статистический анализ временных параметров диграфов – последовательного нажатия двух клавиш (рис. 1).



XH – клавиша «X» нажата;
XO – клавиша «X» отпущена;
YH – клавиша «Y» нажата;
YO – клавиша «Y» отпущена.

Рисунок 1 – Пример диграфа клавиатуры

В ходе мониторинга событий клавиатуры учитываются как алфавитные символы, так и служебные (Shift, Ctrl, Enter, Backspace и т.д.), которые вместе несут уникальную характеристику клавиатурного почерка каждого субъекта. Анализ диграфов событий клавиатуры не требует набора фиксированного образца текста, так как накопление статистики происходит при любых событиях клавиатуры.

Повысить точность аутентификации личности без увеличения объема обрабатываемых данных (т.е. без перехода к триграфам/n-графам) возможно при анализе отношений временных параметров диграфов, т.е. вместо 3-х параметров $t_{X\text{н}Y\text{н}}$, $t_{X\text{о}Y\text{н}}$ и $t_{X\text{о}Y\text{о}}$ (см. рис.1) диграфа «XY» использовать их отношения:

$$\Delta t_{\text{нн\_он}} = \frac{t_{X\text{н}Y\text{н}}}{t_{X\text{о}Y\text{н}}} \quad \text{и} \quad \Delta t_{\text{оо\_он}} = \frac{t_{X\text{о}Y\text{о}}}{t_{X\text{о}Y\text{н}}}. \tag{1}$$

В данном случае профиль клавиатурного почерка субъекта для диграфа «XY», который повторился при наборе M раз, будет иметь следующий вид:

$$T_1 = \begin{vmatrix} \Delta t_{1\ \text{нн\_он}} \\ \dots \\ \dots \\ \Delta t_{\text{M нн\_он}} \end{vmatrix}, \; T_2 = \begin{vmatrix} \Delta t_{1\ \text{оо\_он}} \\ \dots \\ \dots \\ \Delta t_{\text{M оо\_он}} \end{vmatrix}. \tag{2}$$

Далее вычисляются статистические параметры: математические ожидания $m_{T1,}m_{T2,}$ и дисперсии $\sigma^2_{T1,}\ \sigma^2_{T2}$ диграфа.

Итоговый профиль набора представляет собой некоторый вектор E, который состоит из наборов четырех параметров, характеризующих определенное двойное событие клавиатуры:

$$\text{E} = \begin{vmatrix} m_{1\,T1} & \sigma^2_{1\,T1} & m_{1\,T2} & \sigma^2_{1\,T2} \\ m_{2\,T1} & \sigma^2_{2\,T1} & m_{2\,T2} & \sigma^2_{2\,T2} \\ \dots & \dots & \dots & \dots \\ m_{L\,T1} & \sigma^2_{L\,T1} & m_{L\,T2} & \sigma^2_{L\,T2} \end{vmatrix}, \tag{3}$$

где L – количество анализируемых диграфов.

Далее профиль клавиатурного набора представляется в виде ассоциативного массива (4), в котором элементами являются идентификаторы всех введенных субъектом двойных событий клавиатуры, а соответствующими значениями – математические ожидания и дисперсии полученных отношений временных интервалов:

$$Profile_i = \{m_{1i}, m_{2i,}\sigma_{1i}^2, \sigma_{2i}^2\},\ i \in (0, L). \quad (4)$$

В формировании профиля участвуют только те диграфы, время введения которых не превышает предельное значение, определяемое для каждого пользователя индивидуально. Это необходимо делать для того, чтобы незапланированные долгие паузы во время набора текста не влияли на профиль.

Входными значениями для системы аутентификации являются векторы фактических значений временных интервалов диграфов, которые затем преобразуются в векторы inp_T_{1i} и inp_T_{2i}:

$$inp\_T_{1i} = \begin{vmatrix} \Delta t_{1\ \text{нн\_он}_i} \\ \dots \\ \dots \\ \Delta t_{N\ \text{нн\_он}_i} \end{vmatrix},\ inp\_T_{2i} = \begin{vmatrix} \Delta t_{1\ \text{оо\_он}_i} \\ \dots \\ \dots \\ \Delta t_{N\ \text{оо\_он}_i} \end{vmatrix},\quad i \in (0, L), \quad (5)$$

где N – количество повторений -го диграфа.

При сравнении с эталоном $Profile_i$ для каждой компоненты векторов inp_T_{1i} и inp_T_{2i} проверяются условия согласно правилу «трех сигм». В результате формируются векторы согласованности S_i:

$$S_i = \begin{vmatrix} S_{i_1} \\ S_{i_2} \\ \dots \\ S_{i_{2N}} \end{vmatrix},\ S_{i_j} = \begin{cases} 1, & \text{если } m_{1i} - 3\sigma_{1i} \le \Delta t_{j\ \text{нн\_он}_i} \le m_{1i} + 3\sigma_{1i}; \\ 0, & \text{иначе;} \end{cases}$$
$$S_{i_{(N+j)}} = \begin{cases} 1, & \text{если } m_{2i} - 3\sigma_{2i} \le \Delta t_{j\ \text{оо\_он}_i} \le m_{2i} + 3\sigma_{2i}; \\ 0, & \text{иначе.} \end{cases} \quad (6)$$

где $j = 1,2, \dots N$.

По норме вектора согласованности S_i принимается решение R_i о подлинности субъекта для i-го диграфа:

$$\begin{cases} \|S\|_i \le Z_{OTK} - \text{отказ} \ \text{ и } \ R_i = 1; \\ \|S\|_i \ge Z_{\text{ДОП}} - \text{допуск} \ \text{ и } \ R_i = 0; \\ Z_{OTK} < \|S\|_i < Z_{\text{ДОП}} - \text{дальнейший анализ.} \end{cases} \quad (7)$$

Значения порогов отказа и допуска принимаются равными $Z_{OTK} = N$ (50 % единиц в векторе S_i) и $Z_{\text{ДОП}} = 1.2N$ (60 % единиц в векторе S_i).

Аналогично правилу (7) выносится решение о подлинности субъекта на основе анализа всех L диграфов:

$$\begin{cases} \|R\| \le 0.5L - \text{отказ;} \\ \|R\| \ge 0.6L - \text{допуск;} \\ 0.5L < \|R\| < 0.6L - \text{дальнейший анализ.} \end{cases} \quad (8)$$

С каждой успешной аутентификацией субъекта выполняется обновление биоэталона, что позволяет учесть изменения клавиатурного почерка и соответствующим образом адаптировать систему аутентификации.

Список литературы

1.Deian S, Xiaokui S. Robustness of keystroke-dynamics based biometrics against synthetic forgeries//Department of Electrical Engineering, The Cooper Union, New York, NY 10003, United States, may 2011.

2. Zhong Y., Deng Y. Recent Advances in User Authentication Using Keystroke Dynamics Biometrics.- USA.-2015:Science Gate Publishing.-Chapter 2.-pp. 23-40.

3.Синиця Ю.О. Автентифікація суб'єктів за клавіатурним почерком з використанням диграфів // Международная конференция "Интернет-технологии и программирование компьютерных мобильных систем": Материалы XVII Международного молодежного форума "Радиоэлектроника и молодежь в XXI веке ", том 5. — Харьков, 2013. — с. 167-168.

УДК 004.49

Шляхи подолання проблем у сфері кібербезпеки

Артеменко А.С., студентка 5 курсу, stasja.artem@ukr.net
Науковий керівник – Бобришов О.О., асистент
Кіровоградський національний технічний університет, м. Кіровоград

Дана тема стала актуальною в сучасному світі, де захист інформації в кіберпросторі постає дуже гостро. Кібербезпека все частіше розглядається, як стратегічна проблема держави, комплексно зачіпає економіку країни, в тому числі взаємодію національних розробників програмного забезпечення і систем управління, виробників обладнання для забезпечення ІКТ-інфраструктури, низька ринкова конкурентоспроможність яких призводить до необхідності використання рішень іноземних виробників. На практиці дане явище призводить до стрімкого зростання залежності від іноземних виробників і зниження рівня інформаційного захисту у зв'язку з вимушеним використанням «закритого» програмного і апаратного забезпечення в усіх сегментах інфраструктури як для спеціальних державних відомств, так і для цивільного сектора. Уже найближчим часом залежність від іноземних виробників обладнання та розробників програмного забезпечення може досягти критичного рівня.

Особисті мобільні пристрої співробітників, які використовуються для роботи в корпоративних мережах в рамках програм BYOD (Bring Your Own Device), є однією з головних загроз кібербезпеки бізнесу. Чергове підтвердження цього представила компанія Duo Labs. За даними її дослідження, лише на половині всіх смартфонів від Apple, використовуваних сьогодні в світі в рамках BYOD, встановлена остання версія операційної системи iOS. Це автоматично означає, що інша половина продовжує використовувати ранні версії - в яких існує не менше сотні небезпечних уражень.

Втім, з пристроями на платформі Android все йде ще гірше. Лише кожен п'ятий їх користувач може похвалитися тим, що на його смартфоні або планшеті встановлена остання версія ОС Android Lollipop. Все це разом дозволяє говорити про те, що несвоєчасність поновлення ПО мобільних пристроїв перетворюється в одну з головних загроз кібербезпеки не тільки самих користувачів, але і компаній, в яких вони працюють.

Мобільні додатки масово розкривають дані користувачів. Майже 11% всіх мобільних додатків передають дані користувачів стороннім компаніям. Дослідники проаналізували понад 400 тисяч мобільних додатків для Android, представлених в Google Play Store. Як з'ясувалося, близько 10,8% програм розкривають особисті дані користувачів. Найчастіше додатки відправляють на сервери рекламних мереж інформацію про номери телефонів, IMEI-ідентифікатори, історії дзвінків і місцезнаходження телефону. За даними звіту, бізнес-додатки в три рази частіше розкривають особисті дані користувачів в порівнянні з іншими програмами. Найбільш небезпечними додатками виявилися мобільні ігри - в розважальних програмах в п'ять разів частіше виявлялися небезпечні уразливості.

Витік даних в мобільних додатках є основною проблемою безпеки для користувачів. Ненадійні програми передають персональні дані жертв на сторонні сервери і схильні до вразливостей, що дозволяє хакерам викрасти інформацію.

BYOD-системи, хмарні технології, системи віддаленого доступу до робочих місць відіграють значну роль в наш час. Вони можуть завдати великої шкоди підприємствам. Мобільні пристрої все частіше стають причиною витоку корпоративних даних. Найчастіше такі проблеми виникають внаслідок невмілого управління даними пристроями, за рахунок уразливого програмного забезпечення та погано протестованих бізнес-додатків.

Корпоративні дані, які передаються чи зберігаються на незахищених мобільних пристроях, залишаються на хмарних носіях, що підвищує ризики витоку і захоплення даних. Також до негативних наслідків призводить і установка користувачами нових додатків.

Зрозуміло, що в міру повсюдного впровадження технологій мобільних платежів мобільні пристрої стануть представляти ще більшу цінність. За аналогією з загрозою Firesheep

(перехоплення чужих Wi-Fi-сесій), найімовірніше, з'являться програми для перехоплення платіжної інформації користувачів.

Особливості, які будуть впливати на інформаційну сферу в майбутньому:

- кіберзлочинність і нові шляхи на забезпечення кібербезпеки.
- "інтернет речей".
- нові закони про захист даних, які б змусили компанії переглянути погляди та цілі в цій сфері.
- застосування штучного інтелекту і робототехніки для виконання монотонної роботи.
- мобільні пристрої стануть основним інструментом виконання майже будь-яких завдань.
- поява більшої кількості програм із залученням віртуальної реальності.
- будуть поширюватися персоналізований маркетинг і акції, які будуть керуватися даними про місцезнаходження потенційних клієнтів.
- визнані компанії відчують потужну конкуренцію з боку стартапів.

Надійна і захищена робота мереж передачі даних, комп'ютерних систем і мобільних пристроїв є найважливішою умовою для функціонування держави і підтримки економічної стабільності суспільства. На безпеку роботи ключових інформаційних систем загального користування впливає багато факторів: кібер-атаки, порушення, викликані загрозою фізичної розправи, вихід з ладу програмного та апаратного забезпечення, людські помилки. Перераховані явища наочно демонструють, наскільки сучасне суспільство залежить від стабільності роботи інформаційних систем.

Шляхи подолання проблем у сфері інформаційної безпеки:

1. Створити єдиний координуючий орган у сфері інформаційної безпеки та ІТ.
2. Створити нормативну базу, що відповідає вимогам світових стандартів.
3. Створити галузеві центри реагування на загрози в сфері ІТ-безпеки. Ці центри реагування повинні проводити обмін деталями про атаки на корпоративні і державні ресурси, повинні підтримувати "чорний список" серверів, з яких здійснюються атаки.
4. Нарешті, необхідно налагодити процес освіти і професійної підготовки фахівців в галузі управління ІТ та інформаційною безпекою, яких все ще не вистачає в Україні.

Нові підходи допоможуть бізнесу і державі ефективно реагувати на нові виклики сьогодення. У довгостроковій перспективі поліпшення інформаційної та ІТ-безпеки держави зробить його сильнішим і в геополітичних протистояннях.

УДК 004.056

Высоконадежная аутентификация: требования к базам биометрических образов

Ахметов Б.С., директор ИИТТ, д.т.н., профессор, bakhytzhan.akhmetov.54@mail.ru,
Алимсеитова Ж.К., старший преподаватель,
Картаев А., студент 3 курса ИИТТ
Казахский национальный исследовательский университет имени К.И. Сатпаева, г. Алматы

Для повышения надежности функционирования электронного документооборота в банковской сфере и системе электронного правительства в последние годы активно используются средства биометрико-нейросетевой аутентификации личности. Их основным отличием является возможность многофакторного анализа поступающих данных и принятие решения, с какими угодно малыми вероятностями ошибок. При этом актуальным остается проблема тестирования и сертификации средств биометрико-нейросетевой аутентификации личности.

Доверие к высоконадежным средствам биометрической аутентификации определяется результатами их тестирования, выраженными в форме гарантий производителя, подтвержденных по необходимости сертификационными документами. Каждый акт тестирования средства биометрической аутентификации на биометрических данных одного человека требует определенных затрат времени и иных ресурсов. Одним из основных условий проведения тестирования и получения достоверных результатов статистических исследований является наличие баз естественных биометрических образов [1, 2].

Необходимость создания этих баз состоит в том, что они наиболее полно отражают естественное статистическое распределение биометрических признаков людей. Для тестирования средств биометрической аутентификации необходимы базы биометрических образов, размеры которых должны быть достаточными для подтверждения характеристик тестируемых средств. Для тестирования необходимы базы биометрических образов «Свой» и базы биометрических образов «Чужой».

Естественный биометрический образ человека при биометрической аутентификации проходит преобразования, блок-схема которых приведена на рисунке 1 [1, 2].

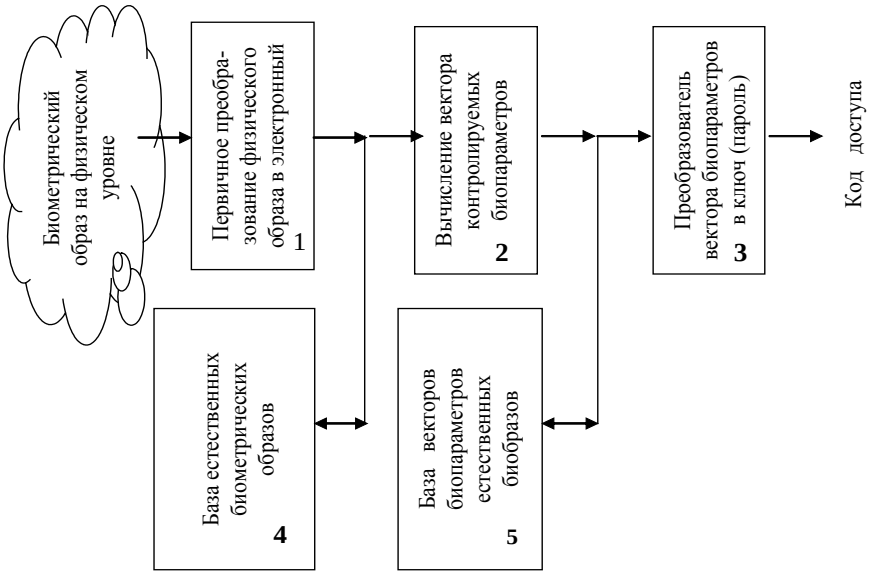


Рисунок 1 – Блок-схема движения информации при биометрической аутентификации

Биометрические образы человека могут быть размещены в соответствующих базах только после их оцифровывания до или после предварительной обработки.

Образы «Свой» отражают статистику распределения биометрических параметров пользователя при его попытках аутентификации. Образы «Чужой» отражают статистику

распределения биометрических параметров злоумышленников, пытающихся нелегально аутентифицироваться.

Базы естественных биометрических образов «Чужой» фрагментируются и классифицируются по их близости к конкретному образу «Свой» и/или конкретному преобразователю биометрия-код, обученному на этом образе «Свой». В качестве меры близости используется расстояние Хэмминга между кодом «Свой» и кодами образов «Чужой».

Базы естественных биометрических образов, предназначенные для тестирования качества работы средств биометрической аутентификации, с биометрическими образами «Свой» разной стабильности, уникальности, качества должны формироваться лицами, уполномоченными осуществлять сертификацию средств аутентификации. Базы для тестирования качества средств биометрической аутентификации должны иметь значительные размеры и располагаться вне этих средств.

Базы естественных биометрических образов «Свой», предназначенные для тестирования средств биометрической аутентификации должны содержать множество примеров различных биометрических образов, принадлежащих разным людям.

Для каждого биометрического образа человека в базе должны быть указаны:

средняя стабильность параметров биометрического образа;

средняя уникальность параметров биометрического образа;

среднее качество параметров биометрического образа.

Приведенные выше данные относительны и должны быть указаны для всех средств, на которых было произведено тестирование, с указанием даты тестирования, тестера, полного названия средства и его производителя.

Базы естественных биометрических образов «Чужой», предназначенные для тестирования средств биометрической аутентификации, должны отражать статистику распределения активного населения (страны, региона) по возрасту, половому признаку, роду занятия, квалификации и иным характеристикам, присущим людям, для которых создано тестируемое средство высоконадежной биометрической аутентификации.

Формирование баз естественных биометрических образов «Чужой» должно осуществляться исходя из десятикратного превышения, находящихся в базе случайных образов «Чужой», по отношению к ожидаемой стойкости к атакам подбора тестируемого средства аутентификации. Прогноз стойкости к атакам подбора (обратной величины вероятности ошибки второго рода) должен осуществляться внутренними средствами тестирования средства аутентификации. Число биометрических образов полной базы вычисляется по формуле:

$$N_{Полн} = \frac{10}{P_2} \ .$$

Список литературы

1 Ахметов Б.С., Волчихин В.И., Иванов А.И., Малыгин А.Ю. Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации: монография. – Алматы: Издательство LEM, 2013. – 152 с.

2. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: монография. – Алматы: Издательство LEM, 2014. – 144 с.

УДК 004.632

Аналіз програмних засобів захисту персональних даних

Білан В.П., студент 5-го курсу
Науковий керівник – Мандрона М.М., старший викладач кафедри управління інформаційною безпекою, канд. техн. наук,
Львівський державний університет безпеки життєдіяльності, м. Львів

Потребу та необхідність захисту особистих даних про особу чітко визначено на законодавчому рівні України [1-3].

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1]. Персональні дані – це вид конфіденційної інформації, що належить до інформації з обмеженим доступом. Отже, система захисту повинна відповідати всім вимогам.

Основною вимогою під час обробки конфіденційної інформації є забезпечення її захисту від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення [2-4].

Головною вимогою для захисту персональних даних, що обробляються в інформаційно-телекомунікаційній системі є наявність комплексної система захисту інформації. Комплексна система захисту інформації – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу [5]. Така система захисту призначена для забезпечення захисту від витоку технічними каналами, для захисту від несанкціонованого ознайомлення та від спеціальних впливів шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Організаційні заходи є обов'язковою складовою для побудови будь-якої системи. Інженерно-технічні заходи здійснюються в міру необхідності.

Основною вимогою до системи захисту персональних даних є забезпечення захисту від несанкціонованого доступу та від комп'ютерних вірусів. Для цього встановлюють комплекси засобів захисту від несанкціонованого доступу (КЗЗ від НСД) [6, 7]. Ці комплекси повинні бути ліцензійні та сертифіковані. Детальний перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, – можна ознайомитись на головній електронній сторінці Держспецзв'язку [8].

Для захисту персональних даних в інформаційно-телекомунікаційній системі потрібно використовувати комплекс із переліку нижче:

- Комплекс засобів захисту інформації від несанкціонованого доступу „Гриф" версії 3;
- Комплекс засобів захисту захищеного носія даних електронних ідентифікаційних та реєстраційних документів на базі чипа InfineonSLE78CLFX4000P;
- Комплекс засобів захисту інформації від несанкціонованого доступу на базі операційної системи Open BSD, шифр "BBOS™" виробництва ТОВ "АТМНІС";
- Захищений від несанкціонованого доступу компонент "Мережевий криптомодуль "Гряда-301" та"Гряда-61";
- Захищений від несанкціонованого доступу компонент "Електронний ключ "Кристал-1Д" та Кристал-1";
- Комплекс засобів захисту інформації від несанкціонованого доступу програмного продукту Symantec Data Loss Prevention11.X виробництва "Symantec", США;
- Захищений від несанкціонованого доступу компонент "Система електронного документообігу АСКОД. Програмне забезпечення АСКОД Корпоративний"
- Пристрої мережевої безпеки FortiGate (20C, 30D, 40C, 50B,60C, 60D, 70D, 80C, 80D, 90D, 92D, 94D, 98D, 110C, 111C, 100D, 140D, 200A, 200B, 224B, 200D, 240D, 280D, 300A,

310B, 300C, 300D, 500D, 700D, 900D, 620B, 600C, 800, 800F, 800C, 1000C, 1000D, 1240B, 1500D, 3016B, 3040B, 3140B, 3240C, 3200D, 3600C, 3700D, 3800D, 3810A, 3180D, 3950B, 5020, 5060, 5140B, 5001C, 5001C, 5001B, 5001D, 5101C) виробництва компанії Hewlett Packard, США;

- Програмний комплекс захисту інформаційних ресурсів "Bitdefender Security for Endpoints" версії 5.x (для платформи віртуалізації Microsoft Hyper-V) виробництва компанії Bitdefender SRL, Румунія.

Перелік сертифікованого антивірусного програмного забезпечення:

- Програмне забезпечення антивірусного захисту "Zillya! Антивірус для Бізнесу" версії 1.1.xxxx.y, Україна;
- Програмний продукт антивірусного захисту інформації ESET File Security для Microsoft Windows Server версії 6.0.X (EFSW) та інші версії виробництва компанії "ESET", Словаччина;
- Комплекс засобів захисту програмного забезпечення антивірусного захисту інформації Symantec Endpoint Protection 12.X, виробництва компанії "Symantec", США;
- Сервіси безпеки програмного комплексу антивірусного захисту "McAfee Complete Endpoint Protection Enterprise Suite" виробництва компанії McAfee Inc., США.

Висновки. У роботі проаналізовано комплекси засобів захисту від несанкціонованого доступу, які входять до складу системи захисту персональних даних. Варто зазначити, що порушення вимог законодавства щодо захисту персональних даних, тягне за собою накладення штрафу від 5100 до 17 000 грн., відповідно до Кодексу України про адміністративні правопорушення.

Список літератури

1. Конституція України. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к /96-вр.

2. Закон України «Про захист персональних даних: від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – С. 481.

3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": від 27.03.2014 N 1170-VII.

4. Білан В.П. Вимоги законодавства щодо захисту персональних даних / В.П. Білан, М.М. Мандрона // Захист інформації в сучасному суспільстві: матер. 1 Міжнародної наук.-техні. конференції, 21-22 листопада 2014 р. – Львів: Вид-во ЛДУ БЖД, 2014. – С. 15-16.

5. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБ України від 08.11.2005 № 125 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

6. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 з останніми змінами згідно ПКМУ № 938 від 07.09.2011.

7. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.

8. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat_id=39181.

УДК 004.056.53

Вплив систем аналізу та досліджень соціальних мереж на сучасне суспільство

Бісюк В.А., викладач, kntubisuk@ukr.net
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Соціальні мережі в сучасному суспільстві поступово розширюють свій функціонал. Перша соцмережа Facebook дозволяла лише зберігати власні фотографії та обмінюватися текстовими повідомленнями, але зараз соцмережі об'єднують величезну кількість користувачів і виконують функції збереження особистих даних, обміну різного роду медіаконтентом і новинами, згруповують користувачів за інтересами і т.д. Однією з важливих функцій соцмереж є донесення інформації до широких мас. Досить часто органи ЗМІ поширюють інформацію, посилаючись на новини, що з'явилися в соціальних мережах або використовують фотографії та відеоролики викладені користувачами. Стало актуальним швидке донесення короткої інформації. Люди не хочуть читати довгі статті чи переглядати телевізійні випуски новин, замість цього вони переглядають короткі топіки інформації в стрічках, або обмінюються новинами в соцмережах.

Але нажаль соцмережі все більше використовуються і для таких зовсім «недитячих розваг», як маніпулювання суспільною думкою, розповсюдження недостовірної або «відретушованої» інформації, провокування та стравлювання окремих верств чи груп користувачів, шпигунство і т.д. Ґрунтуючись на спостереженнях ми змушені констатувати, що соцмережі стають ще одним засобом інформаційних війн.

Об'єкт дослідження – соціальні мережі необхідно представляти, як складову підсистему суспільства, на яку в тій чи іншій мірі впливають і в свою чергу піддаються її впливу суб'єкти і фактори інформаційного впливу (рис. 1).

Дослідження, а особливо прогнозування процесів, які відбуваються в соціальних мережах значно ускладнено через нелінійний характер взаємодії різних складових підсистем суспільства. Крім того неможливо повністю передбачити реакцію складових підсистем і суспільства в цілому на вплив зовнішніх факторів. Так деякі події можуть викликати сильний резонанс і інформація про них широко розповсюджується в соціальних мережах, а деякі можуть відбуватися майже не поміченими через особливості менталітету або уподобання конкретної групи чи поточну політичну або економічну ситуацію.

Розрізняють системи моніторингу та аналізу соцмереж.

Системи моніторингу виконують збір та структурування первинних даних. Виконуються збір та фільтрація текстів, відслідковуються зв'язки між користувачами, об'єднання в «групи» чи «співтовариства», посилання на зовнішні ресурси, цитування інших джерел інформації, розповсюдження окремих даних. Особливо популярні системи моніторингу, що працюють в режимі реального часу, вони набагато складніші в реалізації, ніж ті що використовують ретроспективний збір даних, але їх актуальність результатів їх роботи значно підвищує їх цінність.

Системи аналізу соцмереж виконують більш складну обробку даних, яка може виконуватись в декілька послідовних етапів. Первинні дані в системах аналізу можуть бути отримані з систем моніторингу, або збиратись власне з соцмереж.

Якщо результати моніторингу можуть відповісти лише на прості кількісні запитання, то результати аналізу дають більш глибоке розуміння процесів, які відбуваються в даній соцмережі (або декількох соцмережах одночасно) та дозволяють виявляти статистичні та структурні закономірності в конкретних частинах соцмережі або в системі в цілому.

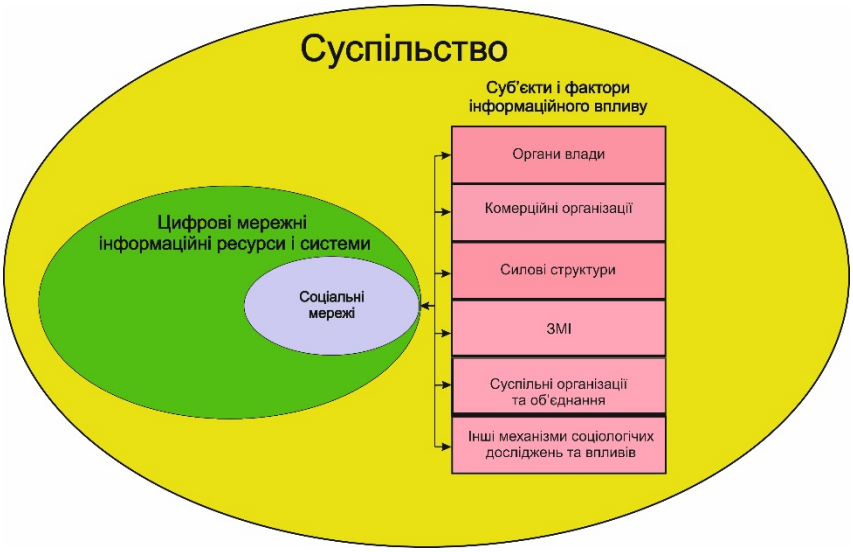


Рис. 1 – Складові підсистеми суспільства

Широко впроваджуються системи прогнозування подій в інтернет-співтоваристві в тому числі в соцмережах. Тут можуть використовуватися статистичні дослідження та моделі динамічних процесів на графах (поширення епідемій, каскадна поведінка) [1]. Наприклад Google Flu - відомий приклад ефективності «великих даних»: сервіс «знаходить» епідемії грипу швидше медиків, аналізуючи статистику запитів у пошуковій системі Google. Механізм дії простий: хворі, або ті хто боїться захворіти, шукають в інструкції до ліків, опис симптомів та іншу інформацію, пов'язану з грипом. Під час епідемій число запитів зростає.

Найбільший інтерес до систем дослідження та прогнозування соцмереж виявляють великі комерційні організації (банківські установи, виробничі корпорації, торгівельні мережі). Моніторинг і аналіз інформації в соцмережах стає невід'ємною частиною ведення бізнесу, від результатів досліджень іноді залежить вибір стратегії розвитку компанії або рекламної кампанії. Особливо комерційні структури зацікавлені в системах, що дозволяє в режимі реального часу проводити автоматичний збір і аналіз інформації в соціальних мережах, а також моделювати і прогнозувати процеси, що відбуваються в соцмережах.

Другим зацікавленим користувачем є органи державної влади та силові структури держави. Перші вивчають реакцію суспільства на ті чи інші владні рішення та процеси, що відбуваються у внутрішньому чи зовнішньому політичному житті, а також намагаються сформувати потрібні їм настрої та вподобання шляхом інформаційного впливу. Силові структури більше зацікавлені в попередженні та протидії інформаційним загрозам, крім того спеціальні засоби можуть допомогти виявити навіть планування терористичних актів або злочинів.

Висновки. Як бачимо широке впровадження та розвиток засобів аналізу та досліджень соціальних мереж відкриває нові широкі можливості для формування та внесення глибоких змін в життя суспільства.

Список літератури

1. Список систем анализа социальных медиа [Електронний ресурс]. – URL: Режим доступу: http://wiki.kenburbary.com (дата звернення 27.01.2016).

2. ADAMIC L., GLANCE N. The Political Blogosphere and the 2004 U.S. Election: Divided They Blog // Proc. of the 3 rd ACM international workshop on Link discovery, 2005. – P. 36–43

3. Литвинова С. Г. Віртуальні спільноти у дослідженнях зарубіжних вчених / С. Г. Литвинова // Інформаційні технології і засоби навчання. – 2012. – № 5 (31). [Електронний ресурс]. – Режим доступу до журналу: http://www.journal.iitta.gov.ua. – Назва з екрана.

УДК 343.98:341.48:004.02

Один з аспектів боротьби з кібертероризмом у всесвітній павутині

Бобришов О.О., асистент, bobrushovoo@i.ua
Кіровоградський національний технічний університет, м. Кіровоград

В результаті стрімкого технічного прогресу людство набуває не тільки безліч шляхів розвитку світового співтовариства, а також нові труднощі та глобальні загрози. З появою та впровадженням в усі сфери діяльності людини всесвітньої мережі Інтернет, виникає таке явище як кібертероризм. І чим більше людина, або її сфера діяльності залежить від всесвітньої мережі, тим більша загроза з боку кібертероризму.

Кібертероризм - це багатогранний феномен, обумовлений багато в чому безконтрольним використанням глобальних мереж, а також недостатньою увагою з боку держави, громадянського суспільства і спецслужб до даного сегменту інформаційного простору.

У 1986 р. у Парижі групою експертів Організації економічного співробітництва і розвитку було вперше дано кримінологічне визначення комп'ютерного злочину, під яким розумілася будь-яка незаконна, неетична або недозволена поведінка, що стосується автоматизованої обробки або передачі даних. Після чого почалася всесвітня боротьба з кібертероризмом.

З 1985 по 1989 р. Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, виробив Рекомендацію № 89, затверджену комітетом Міністрів ЄС 13.09.1989 року. Вона містить список правопорушень, рекомендований країнам - учасницям ЄС для розробки єдиної карної стратегії, пов'язаної з комп'ютерними злочинами.

У 1990 році VIII Конгрес ООН з попередження злочинності і поводження з правопорушниками ухвалив резолюцію, що закликає держави - члени ООН збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності. В квітні 1995 р. було проведено I Міжнародну конференцію Інтерполу з комп'ютерної злочинності. У 1996 році країнами G8 було прийнято рішення про створення спеціальної підгрупи по боротьбі з міжнародними злочинами у сфері високих технологій –"Ліонська група".

У 1997 році міністри внутрішніх справ і міністри юстиції Великої Вісімки на зустрічі у Вашингтоні прийняли «Десять принципів боротьби з високотехнологічними злочинами», що включають, у тому числі, положення про те, що «для тих, хто зловживає інформаційними технологіями, не повинно бути ніяких зон безпеки».

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 року у Будапешті Конвенція Ради Європи про кіберзлочинність. Це один з найважливіших документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний документ такого рівня. В Україні цю конвенцію ратифікували 7 вересня 2005 року.

У 2007 році в Україні створено CERT-UA (Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України) – спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). CERT-UA з 2009 року була акредитована у FIRST (Forum for Incident Response and Security Teams – Форум команд реагування на інциденти інформаційної безпеки).

Як видно з приведеного вище матеріалу проблемі кібертероризму на протязі всього розвитку комп'ютерних та мережевих технологій приділяється значна увага. Але проблема йде у ногу з всесвітнім прогресом і динамічно розвивається.

Шляхами подолання проблеми може бути використання нової моделі всесвітньої павутини, в основу якої взята думка відмови від анонімності користувачів, яка зараз пропонується та заохочується у сучасній світовій мережі Інтернет. Так як анонімність є безкарність. А також створення чіткої координації зусиль усіх ланок та підготовка кваліфікаційних фахівців по боротьбі з кібертероризмом.

Приведені шляхи можуть не бути вирішеням проблеми, але хоча б зрушать чашу терезів у бік кібербезпеки.

Список літератури

1. Бізнес та безпека [Електронний ресурс]. – Кібертероризм та захист персональних даних: http://bsm.com.ua/company-news/kiberbezopasnost/item/132-kiberterrorizm-i-zashchita-personalnykh-dannykh
2. Про ратифікацію Конвенції про кіберзлочинність: закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. - 2006. - № 5-6. - Ст. 71
3. Державне управління: удосконалення та розвиток [Електронний ресурс]. - Організаційні та нормативно-правові засади боротьби з кіберзлочинністю: http://www.dy.nayka.com.ua/?op=1&z=715
4. Інформація і право [Електронний ресурс]. – Міжнародно-правове співробітництво у сфері подолання кіберзлочинності: http://ippi.org.ua/sites/default/files/14sydspk

UDC 681.5

Functional stability as the dominant description of information security systems

Vialkova V., PhD, Taras Shevchencko National University of Kyiv
veravialkova@gmail.com

The implementation of functional stability is achieved by using existing kinds of redundancy through the redeployment of resources to parry the consequences of emergency situations. What is special, in the design phase an additional redundancy should not be administered, and the parrying of the consequences of emergency situations is carried out by redistribution of existing resources. Features of the principle of many complex technical systems led us to make a conclusion, that in spite of the existing major scientific results of the theory of functional stability, the studied mathematical models of complex systems are not able to describe the operation of existing systems adequately [1].

Known properties of complex technical systems, such as stability, reliability, survivability and fault tolerance characterize the systems functioning under the influence of failures and damages. But they do not completely allow describing the processes of functioning in conditions of considerable damages, impact of failures flow and malfunctions, possible terrorist actions and mistakes of operators, and other internal and external destabilizing influences. Therefore, it is advisable to provide a new dominant description of complex technical systems - functional stability for the information security system.

An analysis of known scientific provisions of the existing functional stability theory suggested a conclusion about a lack of publication in explicit look regarding addressing sustainable creating an information security system with functional stability [2,3].

So, to develop and implement the IT in Ukraine, there is an actual common issue of improving an efficiency of ISS, for which the system's properties of functional stability is an important partial problem. Analysis of functional requirements during the creation of a stable system made us find a contradictory situation, which is the aggravation of contradictions between the requirements:

- between the requirement to improve efficiency, which requires additional expenses, and the requirement to reduce the costs through the creating and upgrading;
- between the requirement to reduce time for modernization, that reduces system's efficiency, and the requirement for increased efficiency.

This contradictory situation is the basis of a new relevant scientific problem of providing a dominant description of functional stability of information security systems.

References

1. *Kravchenko Yu., Mikus S. The current state and development of the theory of functional stability // Scientific Papers of Pukhov Institute for Modelling in Energy Engineering. – K.: IPME, 2013. – Vol. 68. – pp. 60-68.*

2. *Buslenko N., Kalashnikov V., Kovalenko I. Lectures on the theory of complex systems. – M.: Sov. Radio, 1973. – 440 p.*

3. *Nedilko S. Basic theory of functional stability of automated air traffic control system. – Kirovograd: DLAU, 2011. – 220 p.*

УДК 004.056.53(044)

Криптографічний захист інформації на базі алгоритму AES

Галата Л.П., асистент кафедри КСЗІ, lili-lili@bigmir.net,
Локтіонова Б.О., студентка 4 курсу НН ІКІТ
Національний авіаційний університет, м. Київ

В даний час для забезпечення конфіденційності інформації інтенсивно використовуються криптографічні методи. Постає необхідність розробки програмного продукту для надійного криптографічного перетворення інформації. Сучасні криптосистеми можна однозначно розділити за способом використання ключів на криптосистеми з закритим ключем (симетричні) і з відкритим ключем (асиметричні).

Advanced Encryption Standard (AES), також відомий під назвою Rijndael - симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий в якості американського стандарту шифрування урядом США. Стандарт почав діяти з 2002 р. і є одним із найпоширеніших, найпродуктивніших і найпростіших в реалізації алгоритмів симетричного шифрування.

Мета роботи – розробка програмного продукту для надійного криптографічного перетворення конфіденційної інформації за допомогою алгоритму AES.

Даний алгоритм перетворює один 128-бітний блок інформації, використовуючи секретний ключ. Для дешифрування отриманого 128-бітного блоку зашифрованої інформації, використовують зворотнє перетворення з тим же ключем. Тому розмір блоку завжди дорівнює 128 біт. Довжина ключа також має фіксований розмір. AES – симетричний алгоритм блочного шифрування використовує ключі у 128/192/256 біт. Якщо він дорівнює 128 біт, то шифрування (дешифрування) відбувається за 10 раундів, якщо 192 біт - 12, а якщо 256 - 14 раундів. Для розшифрування тексту всі криптографічні перетворення, що були використані, можуть бути конвертовані в зворотному порядку. Всі раунди, окрім останнього, ідентичні. В алгоритмі розшифрування послідовність перетворень відрізняється від порядку операцій шифрування, а алгоритм розширення ключа залишається незмінним. В цьому і полягає його симетричність.

У даному програмному продукті було реалізовано AES з розміром ключа в 128 біт, чого цілком вистачає для захисту даних. Агенство Національної Безпеки США використовує саме такий різновид AES для забезпечення безпеки конфіденційних документів: аж до рівня SECRET застосовується шифрування з ключем довжиною в 128 біт. При такій довжині ключа процес шифрування складається з 10 раундів.

Основним елементом, яким оперує алгоритм AES, є байт – послідовність 8 біт, що обробляються як єдине ціле. Для формування байтів 128-бітного блоку відкритого тексту і ключа шифру діляться на групи по 8 біт так, щоб в цілому вийшов масив байт. Проста трансформація виконує циклічний зсув вліво на 1 елемент для першого рядка, на 2 для другого і на 3 для третього. Нульовий рядок не зрушується.

Для ключа алгоритму AES зазвичай використовується заздалегідь визначена конкретна комбінація символів, що має розмір у 128/192/256 біт, але в даному програмному продукті можна використовувати ключ будь-якої довжини. Оскільки після перетворення хеш-функції MD5 блок даних якої завгодно довжини завжди буде мати розмір 128 біт, тому було вирішено використати саме MD5 для наданню ключа фіксованої 128-бітної величини. Завдяки цьому немає необхідності заздалегідь визначати ключ за певним розміром і це спрощує роботу з шифрування (дешифрування).

Також вибір даного криптографічного алгоритму для розробки програмного продукту був обумовлений його підвищеною стійкістю до атак. Безпека AES (Rijndael): для трьох варіантів ключів повний перебір усіх можливих варіантів вимагає 2^{127}, 2^{191} або 2^{255}операцій відповідно. Навіть найменша кількість з цих операцій свідчить, що атака з використанням перебору на

сьогодні не є практично виправданим. Відповідно до оцінок розробників шифр стійкий проти таких видів криптоаналітичних атак:

- диференціального криптоаналізу;
- лінійного криптоаналізу;
- криптоаналізу на основі пов'язаних ключів (слабких ключів в алгоритмі немає).

Алгоритм має не тільки дуже високу захищеність, а й високу швидкість шифрування.

На сучасному рівні засобів і систем криптоаналізу даний програмний продукт на основі шифру AES (Rijndael) забезпечує реальну стійкість і безпеку, також він має прийнятну складність криптографічних перетворень і може бути реалізований для комп’ютерних систем різних класів.

Список літератури

1. Nechvatal J., Barker E., Bassham L., Burr W., Dworkin M., Foti J., Roback E. Report on the Development of the Advanced Encryption Standard (AES). // http://csrc.nist.gov — National Institute of Standards and Technology.
2. Nechvatal J., Barker E., Dodson D., Dworkin M., Foti J., Roback E. Status report on the first round of the development of the advanced encryption standard. // http://csrc.nist.gov — National Institute of Standards and Technology.
3. Панасенко С.П., Батура В.П. Основы криптографии для экономистов: учебное пособие. Под ред. Л.Г. Гагариной. — М.: Финансы и статистика, 2005. — 176 с.

УДК 004.056.53

Огляд методів аналізу соціальних мереж з точки зору інформаційної безпеки держави

Гермак В.С., аспірант, germak_vs@ukr.net
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Сучасний рівень розвитку науки і техніки сприяє підвищенню обсягу і швидкості поширення інформації, та водночас разом з цим загострюються контури нових міжнародних проблем. Передусім це стосується сфери інформаційної безпеки та інформаційного протиборства. В зв'язку зі складнощами, в першу чергу політичними та економічними, до яких в сучасних умовах призводять спроби ведення прямих бойових дій із застосуванням зброї масового ураження, все більшого значення набувають інформаційні війни. При цьому на перший план як арена інформаційного протиборства виходить мережа Інтернет, де не останню роль відіграють он-лайнові соціальні мережі, які надають можливість спілкуватись незважаючи на відстані і час. Тому соціальні мережі стають суттєвим інструментом інформаційного впливу, в тому числі в цілях маніпулювання особистістю, соціальними групами та суспільством в цілому. Це призводить до зростання популярності соціальних мереж як засобів ведення інформаційних війн, і тут вже виникають питання інформаційної безпеки.

Безконтрольне або злочинне використання соціальних мереж як джерела інформаційного впливу призводить до виникнення загроз національній безпеці України шляхом створення негативного інформаційного впливу на свідомість і поведінку громадян та формування спільнот, думки та спрямування яких протирічать ключовим моментам державної політики та підривають політичний лад в країні зсередини. В зв'язку з цим дуже актуальними стають проблеми моделювання та аналізу соціальних мереж з точки зору здійснення впливу на суб'єкти соціальної мережі та реалізації протидії таким впливам.

При аналізі соціальних мереж можна виділити чотири основні методи досліджень: структурний, ресурсний, нормативний і динамічний [1,4].

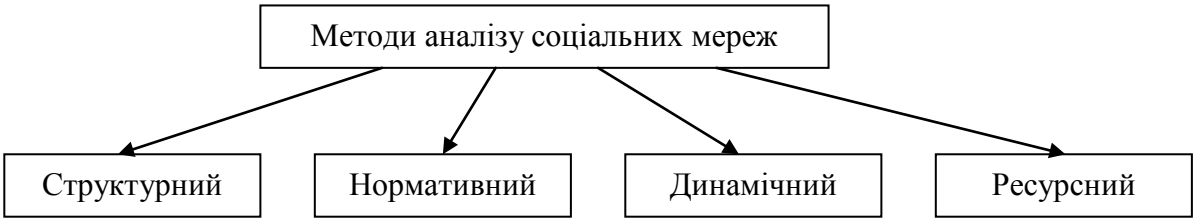


Рисунок 1 – Основні напрямки аналізу соціальних мереж

При структурному підході основна увага приділяється геометричній формі мережі і інтенсивності взаємодій, досліджуються такі характеристики, як взаємне розташування вершин, центральність, транзитивність взаємодій. Структурний аналіз і аналіз поведінки зв'язків в соціальних мережах необхідний для того, щоб визначити найбільш важливі вершини, зв'язки, співтовариства і регіони мережі, що розвиваються. Такий аналіз дозволяє здійснювати огляд глобальної еволюційної поведінки мережі. При структурному аналізі і аналізі поведінки зв'язків використовуються методи статистичного аналізу, визначення співтовариств, алгоритми класифікації. Велике значення надається визначенню співтовариств в соціальних мережах.

Ресурсний підхід розглядає можливості учасників по залученню індивідуальних і мережевих ресурсів для досягнення певної мети і диференціює учасників, що знаходяться в ідентичних структурних позиціях соціальної мережі, по їх ресурсах. В якості індивідуальних ресурсів можуть виступати знання, престиж, багатство, раса, стать. Під мережевими ресурсами розуміються вплив, статус, інформація, капітал. До задач ресурсного підходу відносяться задачі пошуку в мережі експертів та брокерів. Ці задачі є дуже важливими з точки зору організації

протидії інформаційним впливам, так як вони дозволяють визначати впливових учасників мережі, які вносять найбільший вклад у формування суспільної думки рядових учасників мережі.

Нормативний напрям вивчає рівень довіри між учасниками, а також норми, правила і санкції, що впливають на поведінку учасників в соціальній мережі і процеси їх взаємодій. В цьому випадку аналізуються соціальні ролі, які пов'язані з даним ребром мережі, наприклад, відношення керівника і підлеглого, дружні або родинні зв'язки. Комбінація індивідуальних і мережевих ресурсів учасника з нормами і правилами, що діють в даній соціальній мережі, утворює його «мережевий капітал». У спрощеному вигляді «мережевий капітал» можна розглядати як суму деяких переваг, які учасник може отримати в довільний момент часу для досягнення деякої мети.

Динамічний підхід – напрям у вивченні соціальних мереж, в якому об'єктами досліджень є зміни в мережевій структурі з часом: з'являються нові учасники, деякі учасники припиняють взаємодію, виникають нові зв'язки, деякі зв'язки застарівають, оскільки учасники перестають взаємодіяти. Це приводить до змін в структурі соціальних мереж в цілому і в окремих співтовариствах. При цьому виникають питання: з яких причин зникають і з'являються ребра мережі, як мережа змінює свою структуру при зовнішніх впливах, згідно яким законам відбуваються довгострокові зміни між крупними співтовариствами в соціальних мережах, чи існують які-небудь стаціонарні конфігурації соціальної мережі, як розвиваються самі співтовариства в часі, які зміни можуть відбуватися, як можна відстежити і представити їх. Даний напрямок є дуже важливим з точки зору здійснення інформаційного протиборства, так як відтворення результатів у часі є дуже серйозною проблемою при моделюванні інформаційних процесів, зокрема інформаційних операцій.

Отже, сучасні підходи дають змогу розглядати он-лайнові соціальні мережі як складні системи та застосовувати для моделювання цих систем різноманітні методи. Слід зазначити, що загалом лише симбіоз багатьох напрямків може забезпечити реалізацію ефективних, науково обґрунтованих процедур, спрямованих на те, щоб протидіяти маніпулюванню суспільною свідомістю та спробам розхитування політичної та соціальної рівноваги в державі.

Список літератури

1. Чураков А.Н. Анализ социальный сетей // Социологические исследования. - 2001. - № 1. - С. 109-121.

2. Чураков А.Н. Вероятностные модели социальных сетей // Социологические исследования. - 2001. - № 9. - С. 99-114.

3. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства. - М.: Физматлит. - 2010. — 228 с.

4. Батура Т.В. Методы анализа компьютерных социальных сетей // Вестник НГУ - серия "Информационные технологии" - Том 10. - Выпуск 4. - С. 13-28.

5. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. – К.:Інтертехнологія. - 2009. – 164 с.

УДК 004.056.55

Побудова інтелектуальної моделі криптоаналізу шифру Рабіна на базі генетичного алгоритму

Гриник Р.О., викладач, r.grynyk@yandex.ru,
Полотай О.І., ст. викладач, к.т.н., orest.polotaj@gmail.com
Львівський державний університет безпеки життєдіяльності, м. Львів

Алгоритм Рабіна - це асиметрична криптосистема яка використовує відкритий ключ (n) для шифрування повідомлення і закритий ключ (q, n) для розшифрування криптограми. Безпека даної криптосистеми визначається складністю пошуку квадратних коренів по модулю складного числа [6]. Генерування ключів відбувається наступним чином:

- Вибираються пара великих простих чисел (p, q) таких, щоб при діленні на 4 вони давали остачу 3.
- Обчислюється модуль $\mathrm{n} = \mathrm{p} * \mathrm{q}$, який і є відкритим ключем

Крипостійкість алгоритму Рабіна визначається трудомісткістю факторизації великих чисел, тобто для розкриття криптограми необхідно відкритого ключа (n) отримати два простих числа $(p * q)$, тобто задача криптоаналізу зводить до розкладання на множники великого числах.

Перед побудовою інтелектуальної системи для вирішення задачі факторизації необхідно вирішити декілька задач, таких як:

- спосіб представлення хромосоми;
- побудова цільової функції;
- формування початкової популяції;
- вибір (комбінування) генетичних операторів, таких як: вибір батьківських хромосом, схрещення, мутації та селекція.

Структура хромосом. Структура хромосоми являє собою бітову стрічку, котра зберігає інформацію про простий множник, а другий множник знаходиться з $\mathrm{n} = \mathrm{p} * \mathrm{q}$.

Формування початкової популяції. Для формування початкової популяції генерується просте число G випадковим вибором значення бітів, причому останній біт завжди повинен бути рівним одиниці. Коли число згенероване, необхідно визначити середню відстань між простими числа заданого порядку – r.

$$r = \ln(G) = \frac{log_2 G}{log_2 e} = \frac{log_2 G}{1.44265}$$

Знаючи число біт n рівняння приймає наступний вигляд:

$$r = \frac{n}{1.442695} \quad (3)$$

Після обчислення r формується масив чисел в діапазоні $[G - r; G + r]$. Для заданого діапазону будуємо решето Ератосфена. Кожне число $x \in [G - r; G + r]$ послідовно перевіряємо на подільність з простими числами в діапазоні $[2; 2r]$. В даному випадку прості числа в цьому діапазоні необхідно вирахувати заздалегідь, причому будь-яким методом.

Після звуження простору пошуку рішень, до множини можливих рішень, що залишилися застосовуємо тест Міллера-Рабіна [1].

Побудова цільової функції. Декодування хромосоми дає значення першого потенційно простого множника p, для якого є лише один однозначний співмножник. Далі, до отриманого результату застосовуємо імовірнісний тест Міллера-Рабіна з метою отримання інформації про ймовірність простоти числа q. Оскільки кожна хромосома знаходиться в результаті локального пошуку із застосуванням вищевказаного імовірнісного тесту, то можна припустити, що кожний співмножники з певною ймовірністю являється простим. Таким чином, значення цільової функції визначається добутком ймовірностей двох співмножників.

Оператор вибору пари хромосом для створення нової хромосоми. Найбільш ефективним для даної задачі є випадковий вибір батьківських хромосом, оскільки ймовірність того, що $p(q) = 0$ досить висока відповідно і ймовірність того, що цільова функція в цілому для багатьох хромосом в популяції буде дорівнювати нулю, висока, то елітний вибір і «колесо рулетки» будуть призводити до локалізації простору пошуку [2].

Вибір оператора схрещення. У даній роботі застосовувався двоточковий кросинговер. У двоточковому кросинговері хромосоми розглядаються як цикли, які формуються з'єднанням кінців лінійної хромосоми. На даний момент багато дослідників погоджуються, що двоточковий кросинговер кращий, ніж одноточковий [5].

Оператор мутації. Після процесу схрещення відбувається процес мутації. Даний оператор необхідний для «вибивання» популяції з локального екстремуму і перешкоджає передчасній збіжності алгоритму. Це досягається за рахунок того, що змінюється випадково обраний ген в хромосомі.

Селекція. Для створення нової популяції можна використовувати різні методи відбору особин, такі як: елітарний відбір, витіснення, відбір усіканням та інші. Витіснення в даному випадку формує нову популяцію скоріше з віддалених особин, ніж з особин, що групуються близько поточного знайденого рішення. Даний метод найбільш придатний для багато екстремального завдання, при цьому крім визначення глобальних екстремумів з'являється можливість виділити і ті локальні максимуми, значення яких близькі до глобальних [5].

Параметри інтелектуальної системи. Представлена інтелектуальна система характеризується наступними параметрами:

а) кількість популяцій;

б) розмір популяцій;

в) кількість індивідів для вибірки при міграції.

Висновок. Отже, використавши генетичний алгоритм, можна побудувати інтелектуальну модель розкладання великого числа на два простих співмножника, що дає змогу здійснити успішну атаку на криптографічну систему Рабіна знаючи відкритий ключ. Для здійснення успішної атаки необхідно правильно підібрати такі параметри, як кількість популяції та її розмір.

Список літератури

1. Arnault, F. "Rabin-Miller Primality Test: Composite Numbers Which Pass It." Math. Comput.64, 355-361, 1995.

2. David Michael Chan, Automatic Generation of Prime Factorization Algorithms Using Genetic Programming, Stanford Bookstore, 2002.

3. Yitang Zhang, Bounded gaps between primes, Annals of Mathematics 2013

4. Кажаров Х.А. Разработка генетической модели поиска простых чисел для криптоанализа rsa на основе клиент-серверной структуры / Х.А. Кажаров // Известия Южного федерального университета. Технические науки. Т 86, №9, 2008. С. 40-46.

5. Панченко Т.В., Генетические алгоритмы: учебно-методическое пособие/ под ред. Ю.Ю. Тарасевича. — Астрахань : Издательский дом «Астраханский университет», 2007. — 87 с

6. Шнайер Б., Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002. 816 с.

УДК 004.056.53:519.876

Використання методів морфологічного аналізу при проектуванні КСЗІ

Грицюк П.Ю., здобувач, pgrytsiuk1992gmail.com,
Грицюк Ю.І., д.т.н., професор, yurii.i.hrytsiuk@lpnu.ua
Національний університет "Львівська політехніка", м. Львів

Вступ. Головною метою функціонування КСЗІ є досягнення максимальної ефективності захисту об'єктів інформаційної безпеки за рахунок одночасного використання всіх наявних ресурсів, методів і засобів, що загалом унеможливить несанкціонований доступ до інформаційних ресурсів підприємства, та створить належні умови оброблення інформації згідно з чинним нормативно-правовим законодавством України [1].

Кількість завдань, які виникають під час вдосконалення наявних чи розроблення нових КСЗІ, постійно збільшується, водночас значно зростає їхня складність. Здатність передбачити розвиток певних загроз безпеці інформаційних ресурсів підприємства або джерел їх виникнення є істотним чинником при проектуванні нових КСЗІ загалом. Водночас, швидкоплинність розвитку ІТ призводить до того, що під час планування стратегій удосконалення КСЗІ необхідно враховувати не тільки наявні на даний момент проблеми захисту інформації, але й ті, які потенційно можуть виникнути в майбутньому. Одним із потужних методів якісного аналізу роботи наявних і проектованих КСЗІ є методи морфологічного аналізу (ММА) [2].

Методологія морфологічного аналізу складних проблем була розроблена швейцарсько-американським астрофізиком Ф. Цвікі [7], методи якої давали змогу досліджувати повні набори відношень у багатовимірних комплексах задач, які не піддаються розрахунку. У подальшому ці методи були значно розширені, найчастіше використовувалися різними дослідниками для створення та вдосконалення складних технічних систем [3, 6].

Метою застосування ММА при проектуванні КСЗІ є оцінювання всіх альтернатив характерних параметрів так званої морфологічної таблиці з урахуванням зв'язків між ними шляхом експертного їх оцінювання. Отримана інформація потім використовується в процесі реалізації етапів життєвого циклу КСЗІ, зокрема – технологічного передбачення якості та надійності її роботи [5]. Також ММА дають змогу використовувати двоетапну процедуру оцінювання роботи КСЗІ засобами методу стратегій впливу на досліджувану проблему з врахуванням потенційних ризиків і параметра часу [4].

1. Методи отримання початкової інформації. Основним засобом реалізації ММА є морфологічна таблиця, яка складається з N характерних параметрів $\tilde{F} = \{F_j,\ j = \overline{1,N}\}$, що описують об'єкт чи проблему загалом. Кожному характерному параметру F_j відповідає множина альтернатив $\boldsymbol{A} = \{\tilde{A}_j = \{a_{ji},\ i = \overline{1,n_j}\},\ j = \overline{1,N}\}$ його потенційного стану. Отримана з таких елементів конфігурація морфологічної таблиці описує сценарії вирішення проблеми. Для конкретної КСЗІ структура морфологічної таблиці визначається фахівцями з технологічного передбачення на підставі даних, отриманих на етапі попереднього вивчення відповідної проблеми.

Для виконання відповідних розрахунків необхідно отримати початкові ймовірності вибору альтернатив характерних параметрів. Загалом це мають бути незалежні ймовірності, однак для реальних завдань проектування КСЗІ виконання цієї умови практично неможливе, тому для отримання цих величин часто застосовують експертне оцінювання [2].

Рівномірний розподіл. Якщо неможливо апріорно отримати адекватні оцінки ймовірностей вибору альтернатив, або використання експертної процедури не є раціональним через значну невизначеність оцінок або через їх близькість, всім альтернативам надаються однакові значення ймовірностей їхнього вибору: $\boldsymbol{P} = \{\tilde{P}_j = \{p_{ji} = 1/n_j,\ i = \overline{1,n_j}\},\ j = \overline{1,N}\}$. Тоді результат роботи ММА буде базуватись на використанні матриці взаємної узгодженості (див. нижче).

Пряме експертне оцінювання. Для j-го характерного параметра F_j експертами за шкалою Міллера [6, табл. 2] для i-ої альтернативи a_{ji} надається певна оцінка ймовірності її вибору, внаслідок чого матимемо таку їхню множину: $\hat{\boldsymbol{P}} = \{\tilde{\hat{P}}_j = \{\hat{p}_{ji},\ i = \overline{1,n_j}\},\ j = \overline{1,N}\}$. Отримані експертні оцінки для кожного параметра потрібно нормувати:

$$\boldsymbol{P} = \left\{ \tilde{P}_i = \left\{ p_{ji} = \hat{p}_{ji} \Big/ \sum_{k=1}^{n_j} \hat{p}_{jk} \,,\, i = \overline{1, n_j} \right\},\ j = \overline{1, N} \right\}. \quad (1)$$

Експертне оцінювання попарними порівняннями. Для *j*-го характерного параметра F_j експерти оцінюють його стан з точки зору переваги альтернативи a_{ji} над a_{jk}, внаслідок чого отримуємо таку їхню множину: $\tilde{\boldsymbol{\Lambda}} = \{\boldsymbol{\Lambda}_j = \{\tilde{\Lambda}_{ji} = \{\lambda_{jik},\ k = \overline{1, n_j}\},\ i = \overline{1, n_j}\},\ j = \overline{1, N}\}$. Якщо оцінка надання переваги дається на підставі порівняння *i*-ої та *k*-ої альтернатив, то оцінка порівняння *k*-ої та *i*-ої альтернатив має обернене значення $\lambda_{jki} = 1/\lambda_{jik}$. Тоді нормовані значення експертних оцінок ймовірностей вибору альтернатив матимуть такий вигляд:

$$\boldsymbol{P} = \left\{ \tilde{P}_i = \left\{ p_{ji} = \sum_{k=1}^{n_j} \lambda_{jik} \Big/ \sum_{q=1}^{n_j} \sum_{g=1}^{n_j} \lambda_{jqg} \,,\, i = \overline{1, n_j} \right\},\ j = \overline{1, N} \right\}. \quad (2)$$

Той чи інший метод отримання початкової інформації обирають залежно від того, наскільки важливим це є для конкретного завдання проектування КСЗІ. Чим більше залежностей між характерними параметрами морфологічної таблиці, тим менше результат залежить від початкових наближень і, відповідно, можна обирати менш трудомісткі методи. Для більшості задач проектування КСЗІ достатньо прямого експертного оцінювання.

3. Стратегії врахування взаємозв'язків між характерними параметрами. Для врахування зв'язків між параметрами морфологічної таблиці часто використовують числову матрицю взаємної узгодженості [6]. Згідно з розробленою стратегією кожній парі альтернатив a_{ji} і a_{li} характерних параметрів F_j і F_l присвоюється відповідна оцінка $c_{ji;qg} \in [-1,1]$.

Для заповнення матриці взаємної узгодженості експертам пропонуються питання щодо узгодженості кожної пари альтернатив різних характерних параметрів. Кількість питань та їх форма можуть бути різними, однак найчастіше питання ставляться у формі оцінки правомірності висловлювань, що пов'язують відповідні альтернативи. Відповіді експертів переводяться в числову форму за відповідною шкалою, внаслідок чого формується матриця взаємної узгодженості характерних параметрів. Оскільки попарні параметри однаково впливають один на одного, тому заповнюють тільки половину цієї матриці.

Після побудови матриці взаємної узгодженості характерних параметрів [6, табл. 6] вибори тих чи інших альтернатив їхнього стану вже перестають бути незалежними подіями. Це означає, що потрібно знайти такі значення ймовірностей p'_{ji} вибору *i*-ої альтернативи a_{ji} для *j*-го параметра, які б враховували вплив матриці взаємної узгодженості на оцінки альтернатив інших параметрів. Для цього потрібно розв'язати таку систему рівнянь Байєса:

$$\begin{cases} p'_{1,i} = \sum\limits_{i_2=1}^{n_2} \sum\limits_{i_3=1}^{n_3} \dots \sum\limits_{i_N=1}^{n_N} P\left(a_{1,i} \middle| a_{k,i_k},\ k = \overline{2, N}\right) \prod\limits_{k=2}^{N} p'_{k,i_k},\ i = \overline{1, n_1}; \\ p'_{ji} = \sum\limits_{i_1=1}^{n_1} \sum\limits_{i_2=1}^{n_2} \dots \sum\limits_{i_{N-1}=1}^{n_{N-1}} P\left(a_{ji} \middle| a_{k\,i_k}, k = \overline{1, N-1}\right) \prod\limits_{k=1}^{N-1} p'_{k,i_k},\ i = \overline{1, n_j},\ j = \overline{2, N-1}; \text{ де } P\left(a_{ji} \middle| \tilde{V}(j)\right) = \\ \sum\limits_{i=1}^{n_j} p'_{ji} = 1,\ j = \overline{1, N}, \end{cases} \begin{cases} 0, & \text{якщо } \bigvee\limits_{q=1}^{N-1} c_{ji;\tilde{V}_q(j)} = -1, \\ p_{ji}, & \text{якщо } \bigwedge\limits_{q=1}^{N-1} c_{ji;\tilde{V}_q(j)} = 0, \\ 1, & \text{якщо } \bigwedge\limits_{q=1}^{N-1} c_{ji;\tilde{V}_q(j)} = 1, \end{cases} \quad (3)$$

де: $\tilde{V}_q(j) = \{v_k^{(j)},\ k = \overline{1, N}, k \neq j\},\ q \in N$ – набір альтернатив, набутих усіма параметрами, окрім *j*-го, у зазначеній конфігурації; $c_{ji;\tilde{V}_q(j)}$ – значення матриці взаємної узгодженості для *i*-ої альтернативи *j*-го параметра й альтернативи $\tilde{V}_q(j)$. Вираз $P(a_{ji} | \tilde{V}(j))$ вказує на ймовірність вибору альтернативи a_{ji} за умови, що інші параметри набули ті альтернативи, які перераховані після вертикальної риски. Умовні ймовірності апроксимуються, виходячи з деяких умов.

У системі рівнянь (3) знаходиться Σn_j невідомих, а також $N+\Sigma n_j$ рівнянь ($\forall j \in N$). Для кожного параметра одне з рівнянь є надлишковим. Після вилучення цих рівнянь кількість рівнянь і змінних збігатиметься. Також система рівнянь (3) є нелінійною, тому найефективнішими методами її розв'язання є ітераційні методи [5], оскільки система легко зводиться до необхідного вигляду і початкові наближення є достатньо близькими до шуканого розв'язку.

Результатом розв'язання (3) є морфологічна таблиця, що містить значення ймовірностей вибору альтернатив характерних параметрів з урахуванням взаємозв'язків між ними. Ці значення можуть використовуватися для визначення найбільш важливих станів характерних параметрів

задачі проектування КСЗІ, ранжування цих станів за ймовірністю їх виникнення, вибору найбільш імовірних конфігурацій КСЗІ, а також як вхідні дані для подальших методів, зокрема, для другого етапу двоетапної процедури морфологічного аналізу.

У розглянутій вище задачі вважалося, що стани всіх характерних параметрів морфологічної таблиці є невизначеними. Однак під час вирішення деяких реальних проблем проектування КСЗІ часто доводиться досліджувати деякі її стани при конкретних значеннях певних характерних параметрів. У цьому випадку створюється модель виведення "what-if" ("що буде, якщо"). Гнучкість ММА дає змогу зафіксувати будь-який параметр або деяку групу параметрів й отримати розподіли ймовірностей вибору альтернатив для інших параметрів.

Нехай існує підмножина характерних параметрів $\tilde{F}' \subset \tilde{F}$, стан яких зафіксовано, тобто вважається, що поява однієї з альтернатив є гарантованою. Позначимо множину фіксованих параметрів через M, тоді $\tilde{F}' = \{F_{j'},\ j' \in M\}$. Кожному фіксованому параметру $F_{j'}$ відповідає його фіксована альтернатива $a_{j',i'},\ i' \in n_{j'},\ j' \in \overline{1, M}$. Для цієї альтернативи $p_{j',i} = p'_{j',i} = 1$, а для інших альтернатив фіксованого параметра $p_{j',i} = p'_{j',i} = 0$, $i \in n_{j'}, i \neq i', j' \in M, j \neq j'$.

Завдання полягає в тому, щоб дещо змінити систему рівнянь (3) для розрахунку ймовірностей вибору альтернатив характерних параметрів і вилучити з неї рівняння, що відповідають фіксованим параметрам. Внаслідок цього отримаємо таку систему рівнянь Байєса:

$$\begin{cases} \left\{ p'_{1,i} = \sum\limits_{\substack{i_2=1 \\ i_2 \neq j}}^{n_2} \sum\limits_{\substack{i_3=1 \\ i_3 \neq j}}^{n_3} \dots \sum\limits_{\substack{i_{N\cap M}=1 \\ i_{N\cap M} \neq j}}^{n_{N\cap M}} P\left(a_{1,i} \middle| a_{k,i_k},\ k = \overline{2, N\cap M},\ k \neq j\right) \prod\limits_{\substack{k=2 \\ k\neq j}}^{N\cap M} p'_{k,i_k} \right\},\ i = \overline{1, n_1 \cap M}; \\ \left\{ p'_{ji} = \sum\limits_{\substack{i_1=1 \\ i_1 \neq j}}^{n_1} \sum\limits_{\substack{i_2=1 \\ i_2 \neq j}}^{n_2} \dots \sum\limits_{\substack{i_{N-1\cap M}=1 \\ i_{N-1\cap M} \neq j}}^{n_{N-1\cap M}} P\left(a_{ji} \middle| a_{k,i_k},\ k = \overline{1, N-1\cap M},\ k \neq j\right) \prod\limits_{\substack{k=1 \\ k\neq j}}^{N-1\cap M} p'_{k,i_k} \right\},\ i = \overline{1, n_j},\ j = \overline{2, N-1\cap M}; \\ \left\{ \sum\limits_{i=1}^{n_j} p'_{ji} = 1 \right\},\ j = \overline{1, N\cap M}. \end{cases} \quad (4)$$

Розв'язком цієї системи рівнянь будуть ймовірності вибору альтернатив нефіксованих характерних параметрів при обраних альтернативах фіксованих параметрів.

Отже, розроблене математичне і програмне забезпечення ММА дає змогу: будувати модель функціонування КСЗІ, яка базується на її структурі; оцінити ймовірність реалізацій різних її конфігурацій з певними характеристиками; спостерігати за поведінкою КСЗІ, фіксуючи певні її параметри; ранжувати за ефективністю параметрів певні стратегій функціонування КСЗА; оцінювати потенційні ризики для КСЗІ, заданих морфологічною таблицею.

Список літератури

1. Грицюк Ю.І. Особливості реалізації принципу розумної достатності функціонування комплексної системи захисту інформації на підприємстві / Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2015. – Вип. 25.4. – С. 313-324.

2. Згуровский М.З. Системный анализ: проблемы, методология, приложения / М.З. Згуровский, Н.Д. Панкратова. – К. : Изд-во "Наук. думка", 2005. – 743 с.

3. Одрин В.М. Метод морфологического анализа технических систем / В.М. Одрин. – М. : Изд-во ВНИИПИ, 1989. – 312 с.

4. Панкратова Н.Д. Оцінювання багатофакторних ризиків у стратегії розв'язання задач технологічного передбачення / Н.Д. Панкратова, І.О. Савченко // Доповіді НАН України. – 2010. – № 8. – С. 36-42.

5. Панкратова Н.Д. Стратегія застосування методу морфологічного аналізу в процесі технологічного передбачення / Н.Д. Панкратова, І.О. Савченко // Наукові вісті НТУ України "КПІ". – 2009. – № 2. – С. 35-44.

6. Савченко І.О. Методологічне і математичне забезпечення розв'язання задач передбачення на основі модифікованого методу морфологічного аналізу / І.О. Савченко // Системні дослідження та інформаційні технології. – К. : НТУУ "КПІ". – 2011. – № 3. – С. 18-28 с.

7. Zwicky F. New methods of bought and procedure / F. Zwicky, A. Wilson // Contributions to the symposium on methodologies, May, 22-24. – Pasadena. – 1967. – Pp. 273-297.

УДК 004.056.52: 004.891

Передумови створення системи експертного оцінювання шкоди національній безпеці України у разі витоку інформації з обмеженим доступом

Дрейс Ю.О., к.т.н., доцент, DreisYuri@gmail.com
Національний авіаційний університет, м. Київ

В умовах підвищення рівня розвідувальної діяльності іноземних спецслужб та, виходячи з необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, згідно до рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року, одним із завдань є вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України, зокрема, створення спеціальних програмних і технічних засобів захисту державних інформаційних ресурсів (ДІР), вжиття додаткових заходів щодо захисту інформації з обмеженим доступом (ІзОД) під час її обробки в інформаційних системах.

Згідно ст.7 Закону України «Про основи національної безпеки України» однією із основних реальних та потенційних загроз національній безпеці України в інформаційній сфері є розголошення інформації, яка становить державну таємницю (ДТ), або іншої ІзОД, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави.

Так, наприклад, відповідно до ст.1 Закону України «Про державну таємницю» охороні державою підлягають відомості таємної інформації, які визнані ДТ у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці. Відомості становлять ДТ з часу опублікування «Зводу відомостей, що становлять ДТ» (ЗВДТ), до якого вони включені за процедурою прийняття державним експертом з питань таємниць рішення про віднесення цих відомостей до ДТ зі встановленням їх ступеня секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці у разі розголошення відомостей, що становлять ДТ, чи втрати матеріальних носіїв секретної інформації (МНСІ).

Слід зазначити, що здійснення заходів щодо віднесення відомостей до ДТ, засекречування, розсекречування та охорони МНСІ, криптографічний та технічний захист та інші витрати, пов'язані з ДТ, фінансуються за рахунок Державного бюджету України. Тому наявне зростання витрат на заходи охорони ДТ та збитків, що пов'язані з наслідками розголошення ДТ, втратою МНСІ та їх ліквідацією, підвищують вимоги до прогнозування й інформаційно-аналітичної підтримки процесів прийняття рішень щодо забезпечення інформаційної безпеки України при обробці ДІР, особливо ДТ, стосовно:

- удосконалення методичних рекомендацій ДЕТ щодо визначення підстав для віднесення відомостей до ДТ та ступеня їх секретності;
- експертизи матеріальних носіїв інформації на предмет наявності відомостей, що становлять ДТ, та присвоєння їм грифу секретності;
- встановлення строків засекречування та розсекречування МНСІ;
- визначення базових параметрів шкоди національній безпеці України в інформаційній сфері (при розголошенні ІзОД, а саме: ДТ, службової інформації, конфіденційної інформації (зокрема, персональних даних, що обробляються в державних автоматизованих системах));
- організації формування та опублікування ЗВДТ та розгорнутих переліків відомостей, що становлять ДТ (РПВДТ);
- порядку забезпечення режиму секретності суб'єктом режимно-секретної діяльності та режимно-секретним органом (РСО);
- оцінювання ефективності системи охорони ДТ у цілому, обумовлюють необхідність розробки системи оцінювання шкоди національній безпеці у разі витоку ІзОД.

Це саме стосується і до інших видів ІзОД, наприклад до службової інформації, яка на законодавчому рівні не регулюється окремим законом і має слабку нормативно-правову основу, на відміну від персональних даних, що хоча б регулюються законом «Про захист персональних даних».

До недоліків можна віднести те, що в Україні не має жодних держаних розробок, які вирішують завдання оцінювання шкоди національній безпеці у разі розголошення ІзОД чи втрати її матеріальних носіїв, окрім «Методичних рекомендацій…» виданих Держкомсекретів у 1996 року, що на практиці не використовується.

Висновки. Розроблено науково-методологічну основу (базу) [1-11], яка дозволяє створити систему оцінювання шкоди національній безпеці України у разі розголошення таких видів ІзОД як: державна таємниця, службова інформація та конфіденційна інформація (зокрема, персональних даних).

Список літератури

1. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія / Олександр Корченко, Олександр Архипов, Юрій Дрейс. – К.: Наук.-вид. центр НА СБ України, 2014. – 332 с.: іл. ISBN 978-617-7092-26-0

2. Дрейс Ю. Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання / Юрій Дрейс // Безпека інформації. – 2014. – Т. 20, № 2. – С. 176 – 184.

3. Корченко О. Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці / Олександр Корченко, Максим Луцький, Марія Захарова, Юрій Дрейс // Захист інформації. – 2013. – Т. 15, № 1. – С. 14 – 20.

4. Дрейс Ю. Експериментальне дослідження системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці / Юрій Дрейс // Захист інформації. – 2013. – Т. 15, № 4. – С. 337 – 345.

5. Дрейс Ю. Метод нечіткої класифікації відомостей, що становлять державну таємницю за встановленими критеріями / Юрій Дрейс // Вісник Національного університету «Львівська політехніка». – 2013. – № 774 : Автоматика, вимірювання та керування. – Львів : Видавництво Львівської політехніки, 2013. – С. 10–16.

6. Корченко О. Метод аналізу і оцінки величини можливої шкоди національній безпеці держави у сфері охорони державної таємниці / Олександр Корченко, Світлана Казмірчук, Юрій Дрейс // Захист інформації. – 2012. – № 3. – С. 5 – 18.

7. Корченко О. Роль та місце державної таємниці у контексті політико-правового аналізу / Олександр Корченко, Юрій Дрейс // «Захист інформації і безпека інформаційних систем», ІІІ міжнародна науково-технічна конференція: матеріали конференції, 05–06 червня 2014 р. – Львів: НУ «Львівська політехніка», 2014. – С. 12 – 13.

8. Корченко О. Модель оцінювання шкоди національній безпеці в інформаційній сфері / Олександр Корченко, Юрій Дрейс // «Захист інформації і безпека інформаційних систем», ІІ Міжнародна науково-технічна конференція: матеріали конференції, 30 травня – 01 червня 2013 р. – Львів: НУ «Львівська політехніка», 2013. – С. 26 – 28.

9. Корченко О. Розробка системи експертного оцінювання у сфері охорони державної таємниці / Олександр Корченко, Юрій Дрейс // «Актуальні проблеми управління інформаційною безпекою держави», науково-практична конференція: збірник матеріалів, 30 березня 2012р. – К.: Наук.-вид. відділ НА СБ України, 2012. – С. 161 – 164.

10. Дрейс Ю. Врахування інтересів держави в методиці оцінювання шкоди у сфері охорони державної таємниці / Юрій Дрейс // «Інтегровані інтелектуальні робототехнічні комплекси» (ІІРТК-2012): V міжнародна науково-практична конференція: матеріали конференції, 15-16 травня 2012р. – К. : НАУ, 2012. – С. 316 – 318.

11. Дрейс Ю. Основа розробки моделі експертного оцінювання інформації з обмеженим доступом, що є власністю держави / Юрій Дрейс // «Проблеми створення, розвитку, застосування інформаційних систем спеціального призначення», 19 науково-практична конференція: Ч.1: тези доповідей, 19 квітня 2012. – Житомир: ЖВІ НАУ, 2012. – С.158-159.

УДК 004. 056

Інформаційна стійкість соціотехнічних систем в умовах інформаційної війни

Дудатьєв А.В., доц., к.т.н., доц., dudatyev.av@gmail.com
Вінницький національний технічний університет, м. Вінниця

Інформаційна війна або інформаційна протидія може виникати і проводитись на різних рівнях управління інформаційною безпекою – рівні окремого підприємства, рівні окремого регіону, який може включати комплекс об'єктів захисту і на самому високому рівні – рівні держави. При цьому існує залежність інформаційної захищеності між відповідними рівнями системи, що включає елементи " підприємство - регіон – держава ". Для ефективного рішення задачі оцінювання та забезпечення комплексної інформаційної безпеки багаторівневої системи необхідно мати адекватне управління, яке здатне забезпечити комплексний захист інформаційних ресурсів, на відповідному рівні і системи в цілому. У великій кількості випадків, об'єктом проти якого проводяться спеціальні інформаційні операції є соціальна складова соціотехнічної системи (СТС). Саме тому актуальною проблемою є рішення задачі управління комплексною інформаційною безпекою з метою забезпечення стійкого функціонування СТС в умовах інформаційної війни.

Соціотехнічні системи – це системи, порушення стійкості у яких можливо внаслідок різних причин, як внутрішніх так і зовнішніх, зокрема внаслідок проведення спеціальних інформаційно-психологічних операцій (ІПО).

У доповіді запропоновано визначення інформаційної стійкості СТС. Також представлений комплекс математичних моделей, які дозволяють отримати ймовірнісну оцінку поточного стану захищеності соціальної частини соціотехнічної системи з точки зору порушення конфіденційності, цілісності та доступності, а також отримати загальну ймовірнісну оцінку (вектор стійкості) щодо стійкості соціотехнічної системи в умовах проведення спеціальних ІПО. У доповіді також запропонована умова стійкості або ймовірнісний критерій стійкості СТС, який базується на понятті інформаційного мема і порівнянні ймовірності появи одного мема після другого в інформаційному просторі, з ймовірністю обробки мема або часом перетворення нового мема в управляюче рішення.

Координати вектора стійкості за необхідністю можна розкласти на дві складові, що відповідають ймовірнісним оцінкам порушення конфіденційності цілісності або доступності відповідно.

Отриманий результат дозволяє визначити стійкість системи "в малому", тобто визначити стійкий стан СТС, без визначення її меж і визначити стійкість системи "у великому", тобто визначення меж стійкості і фактів відхилень параметрів системи (ймовірності порушення цілісності, конфіденційності та доступності) за відповідні межі. Відповідно задача аналізу стійкості соціотехнічної системи в умовах інформаційного протиборства може быти розділена на такі:

1) чи стійка соціотехнічна система при заданих значеннях параметрів;

2) в яких межах можна змінювати або допускати зміни параметрів соціотехнічної системи, щоб система була у стані стійкості.

Отримані результати щодо аналізу стійкості соціотехнічних систем в умовах інформаційних впливів дозволяє розширити і більш ефективно використовувати НД ТЗІ 2.5 – 005 – 99 "Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД" в сенсі представлення базового профілю захищеності і відповідного гарантування необхідного рівня захищеності. Це у свою чергу дозволить організувати ефективний захист від деструктивних інформаційних впливів, а також реалізувати запропонований підхід щодо комплексного захисту інформаційних ресурсів у структурі інформаційно-аналітичних центрів на рівні управління інформаційною безпекою – "підприємство-регіон-держава".

УДК 621.391

Вдосконалення способу безпечної багатошляхової маршрутизації повідомлення з балансуванням числа його фрагментів за маршрутами

Єременко О.С., докторант, oleksandra.yeremenko@nure.ua,
Добришкін В.Ю., студент, avlem@ukr.net
Харківський національний університет радіоелектроніки, м. Харків

Як показав проведений аналіз, однією з найважливіших задач, яка регламентується стандартами побудови мереж наступного покоління NGN, є завдання реалізації функцій інформаційної безпеки. Відповідно до вимог стандартів Міжнародного Союзу Електрозв'язку (МСЕ) забезпечення інформаційної безпеки здійснюється в рамках трьох рівнів: безпеки інфраструктури, безпеки сервісів і безпеки додатків [1]. При цьому ефективність роботи верхніх двох рівнів цілком і повністю визначається ефективністю функціонування засобів рівня безпеки інфраструктури, основними завданнями якого є: забезпечення безпеки на рівні мережевих елементів (комутаторів, маршрутизаторів, серверів), каналів зв'язку і маршрутів, які вони складають, в цілому.

Як правило, рівень безпеки мережевих елементів оцінюється за допомогою такого важливого показника як ймовірність компрометації, де під компрометацією розуміється факт несанкціонованого доступу до захищеної інформації, а також підозра здійснення такого доступу. Серед існуючих методів забезпечення заданого рівня безпеки можна виділити захищену передачу повідомлення, розділеного на фрагменти і переданого від відправника отримувачу за допомогою багатошляхової маршрутизації з балансуванням числа фрагментів за шляхами, які не перетинаються. У цьому випадку в ході багатошляхової маршрутизації і балансуванні числа фрагментів повідомлення за шляхами необхідно забезпечити заданий рівень мережевої безпеки, представленої імовірністю компрометації переданого повідомлення P_{msg}:

$$P_{msg} \le \gamma_P, \qquad (1)$$

де γ_P – допустима ймовірність компрометації повідомлення в мережі. На сьогодні відомі тільки методики оцінки ймовірності компрометації для випадку використання шляхів, що не перетинаються, тобто для шляхів, в яких загальними є тільки вузли відправник та отримувач [2, 3].

В разі використання відомих аналітичних виразів для розрахунку ймовірності компрометації повідомлення, яке передається частинами за множиною шляхів, що не перетинаються, передбачаються такі вихідні дані:

S_{msg} і D_{msg} – вузли відправник та отримувач повідомлення, що передається;

M – кількість використовуваних шляхів, що не перетинаються, при маршрутизації частин повідомлення;

p_i^j – ймовірність компрометації j-го елемента (вузла, каналу) i-го шляху;

M_i – число елементів в i-м шляху, які можуть бути скомпрометовані.

В ході подальших міркувань вважається, що відправник та отримувач безпечні, тобто ймовірності компрометації вузла-відправника та вузла-отримувача дорівнюють нулю. Крім того, як і в роботах [2-4], вважається, що якщо елемент (вузол, канал) шляху скомпрометований, то всі фрагменти, що передаються через цей елемент, також будуть скомпрометовані. Тоді ймовірність компрометації i-го шляху, що складається з M_i елементів, можна розрахувати за допомогою виразу

$$p_i = 1-(1-p_i^1)(1-p_i^2)\dots(1-p_i^{M_i}) = 1-\prod_{j=1}^{M_i}(1-p_i^j). \qquad (2)$$

Однією з основних умов, яка в обов'язковому порядку повинна виконуватися в ході безпечної маршрутизації, є те, що ймовірність компрометації повідомлення при його передачі по мережі не повинна перевищувати заданого допустимого значення (1). Тоді, наприклад, ймовірність компрометації повідомлення, розділеного на N частин відповідно до схеми Шаміра (N,N) і переданого за M шляхами, визначається виразом [2,4]

$$P_{msg} = \prod_{i=1}^{M} p_i \,. \qquad (3)$$

В свою чергу використання шляхів, які не перетинаються, призводить до неефективного використання мережних ресурсів і зниження якості обслуговування, перш за все за показниками продуктивності.

Таким чином, пропонується вдосконалення існуючого способу безпечної багатошляхової маршрутизації повідомлення з балансуванням числа його фрагментів за маршрутами, причому необхідно вирішити наступне:

1. Розрахунок множини маршрутів між заданими вузлами відправник та отримувач. У роботі [5] з метою підвищення продуктивності телекомунікаційної мережі при багатошляховій безпечній маршрутизації запропоновано задіяти в тому числі і маршрути, що перетинаються за каналами та/або вузлами. При цьому представлена методика розрахунку ймовірності компрометації повідомлення при використанні маршрутів, які перетинаються, з послідовно-паралельною та комбінованою структурою. На ряді числових прикладів проведений аналіз впливу на ймовірність компрометації повідомлення параметрів безпеки окремих елементів (каналів зв'язку) і фрагментів мережі, а також доведено доцільність її використання. В якості методу визначення множини маршрутів, що перетинаються за вузлами, можливе використання моделі, представленої в [6].

2. Фрагментація повідомлення, що передається, відповідно до обраної схеми Шаміра.

3. Розподілення числа фрагментів повідомлення, що передається, між множиною маршрутів, визначених у ході вирішення першого завдання.

Отже запропоноване вдосконалення способу безпечної багатошляхової маршрутизації повідомлення з балансуванням числа його фрагментів за маршрутами розширює застосування існуючих способів з метою підвищення продуктивності телекомунікаційної мережі за рахунок використання маршрутів, що перетинаються за каналами та/або вузлами.

Список літератури

1. ITU-T X-805. Security architecture for systems providing end-to-end communications, 2003.
2. Lou W. SPREAD: Improving Network Security by Multipath Routing in Mobile Ad Hoc Networks / W. Lou, W. Liu, Y. Zhang, Y. Fang // Wireless Networks. – 2009. – Vol. 15, Issue 3. – PP. 279–294.
3. Alouneh S. A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing / S. Alouneh, A. Agarwal, A. En-Nouaary // Computer Networks: The International Journal of Computer and Telecommunications Networking. – 2009. – Vol. 53, Issue 9. – PP. 1530 – 1545.
4. Yeremenko O.S. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET / O.S. Yeremenko, Ali S. Ali // Radioelectronics and Informatics. – 2015. – № 1 (68). – С. 26–29.
5. Еременко А.С. Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной или комбинированной структурой / А.С. Еременко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №6(40) – С. 64-71.
6. Yeremenko O.S. Enhanced Flow-based Model of Multipath Routing with Overlapping by Nodes Paths / O.S. Yeremenko // Second International IEEE Conference Problems of Infocommunications. Science and Technology (PICS&T-2015). Proceedings. – Kharkiv: Kharkiv National University of Radio Electronics. Ukraine, Kharkiv, October 13−15, 2015. – PP. 42-45.

УДК 004.42

Роль мобільних додатків в інформаційних війнах

Єршов В.В., ershowvlad@gmail.com
Кіровоградський державний педагогічний університет, м. Кіровоград

Інформаційні війни вже давно стали невід'ємною складовою протистояння ворогуючих держав. З метою враження інформаційної сфери країни, розпалу політичної та міжнаціональної ворожнечі і поширення сепаратиських настроїв серед населення зовнішньополітичні супротивники України вдаються до застосування технічних засобів, в тому числі програмних додатків під управлінням операційних систем мобільних пристроїв, які на сьогодні наявні практично у кожного громадянина нашої держави – iOS/Android/WP-смартфонів і планшетів. Тому важливо розглянути ряд типових випадків використання мобільних продуктів в контексті ведення інформаційної війни проти України на прикладі конкретних програм – адже поінформованість є запорукою захищеності.

Мобільний застосунок може слугувати надійним та безперебійним джерелом доступу до інформації в умовах, коли ворог намагається обмежити до неї доступ. Так, наприклад, у 2015 році на адресу одного з інтернет-видань, що висвітлювало об'єктивну дійсність життя на тимчасово окупованій території півострова Крим, почали надходити попередження з боку Роскомнагляду з погрозами блокування ресурсу на території Росії [2]. Підставою для вчинення протиправних дій була ніби як "проукраїнська спрямованість діяльності медіа-компанії". Тому, з метою забезпечення доступу населення, передусім на окупованій місцевості, до інформаційних матеріалів керівництвом було прийняте рішення про розробку мобільних додатків для операційної системи iOS (*itunes.apple.com/app/id1025446858*) та Android (*play.google.com/store/apps/details?id=com.moac.android.sobytiyaInfo*), що використовують захищені протоколи передачі даних, тим самим унеможливлюючи блокування та перехоплення інформації.

Крім того, мобільні додатки також доцільно розглядати не тільки як механізм захисту від посягань країни-агресора, але і як інструмент передусім активної фази ведення протистояння. Зокрема, як шляхи поширення новин, в тому числі, пропонованих у телевізійному форматі. Прикладом може слугувати iOS-застосунок "UATV - українське телебачення в інтернеті" (*itunes.apple.com/app/id1076183440*), що надає зручний інтерфейс для перегляду понад 60 найбільш популярних новинних українських телеканалів (включаючи 5 канал, 112 канал та Перший Національний). Опублікувавши додаток у мобільному магазині цифрової дистрибуції iTunes Store, ми отримали можливість донести актуальну, об'єктивну та неспотворену російськими ЗМІ картину подій, що відбуваються на теренах нашої держави, охоплюючи тимчасово окуповані території та зону проведення АТО.

Окремо слід відзначити такий шлях активізації суспільної свідомості як висвітлення національної культури, історії, символіки. Поширення державних символів у мобільних додатках може слугувати засобом привернення уваги аудиторії користувачів мобільних пристроїв, маючи на меті піднесення патріотичного духу населення.

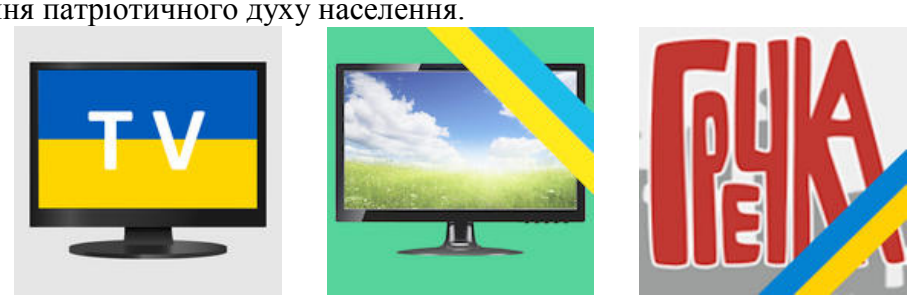


Рисунок 1 – Піктограми ряду iOS-додатків, що містять у своєму складі Державний Прапор України (UkrTV, UATV, Gre4ka.info)

Важливо відмітити, що одним з фронтів гібридної війни зазвичай є фінансово-економічний. Агресор шляхом поширення завідомо неправдивих повідомлень про несприятливі економічні ситуації (на кшталт різкого здорожчання грошових одиниць, інфляцію валюти, ліквідацію банків) у соціальних мережах та інших засобах масової інформації намагається поширити панічні та недовірчі настрої серед населення, таким чином підриваючи довіру до інститутів влади. Тому обґрунтованою є розробка та оприлюднення додатків "Курс гривні - actual rate of Ukrainian currency" (*itunes.apple.com/app/id1086349431*) та подібних, які мають на меті інформування населення про актуальний стан національної валюти та новин фінансового сектору.

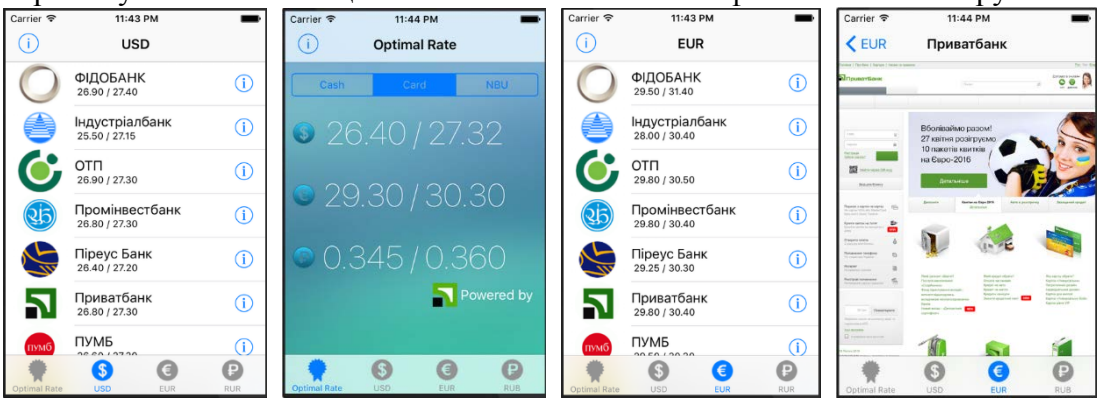


Рисунок 2 – Вигляд екранів програми "Курс гривні"

Слід зазначити, що механізм поширення додатків для магазинів цифрової дистрибуції Apple Store / Google Play / Windows Store передбачає їх доступність для завантаження не тільки на території нашої держави, а й у інших країнах, відтак формує позитивний імідж України в очах світової громадськості а також привертає увагу іноземної спільноти до проблем анексії Криму, самопроголошення терористичних організацій (так званих "ЛНР/ДНР") на Сході України тощо.

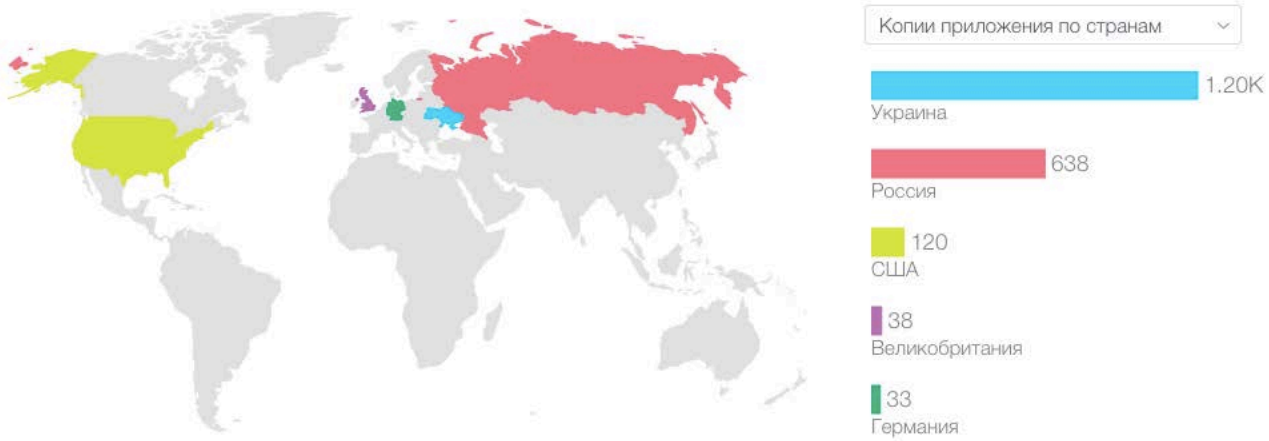


Рисунок 3 – Зображення на карті регіонів з найбільшою кількістю інсталяцій мобільного додатку UATV

Висновки. Можна констатувати, що вже на даному хронологічному етапі мобільні пристрої перетворилися на потужне знаряддя ведення інформаційної війни. З огляду на те, що гібридний тип ведення війни лише поширюється, так само як і зростає відносна частка смартфонів на ринку комп'ютерів, необхідно приділяти належну увагу можливостям даних технологій при створенні планів обороноздатності кожної розвиненої держави.

Список джерел

1. Ілюстрації до статті - продукти автора в Apple Store [Електронний ресурс]. – Режим доступу: itunes.apple.com/developer/id879767497

2. У "Событий Крыма" появилось приложение для смартфонов в Google Play [Електронний ресурс]. – Режим доступу: www.sobytiya.info/news/15/56506

УДК 681.3.07

Програмний емулятор комплексних атак на сервіси протоколу DHCP локальної мережі ETHERNET

Єфіменко А.А., доцент кафедри програмного забезпечення систем, к.т.н., yefim1976@gmail.com,
Власюк О.К., студент 4-го курсу факультету інформаційно-комп'ютерних технологій,
vlasyuk94@gmail.com
Житомирський державний технологічний університет, м. Житомир

Підготовка висококваліфікованих фахівців у сфері захисту інформації в комп'ютерних системах та мережах традиційно передбачає отримання студентами глибоких знань мережних моделей, архітектур, технологій, обладнання, протоколів, операційних систем, а також їх вразливостей та засобів захисту від можливих мережних атак. У той же час ці знання повинні підкріплюватися і відповідними практичними навичками. Традиційно отримання практичних навичок з налагодження та безпечної експлуатації мереж здійснюється з використанням реального обладнання. Такий шлях у більшості випадків є ресурсо- та часомістким і не завжди ефективним. Альтернативою є використання середовищ моделювання роботи мереж, які базуються на симуляційному, емуляційному або комбінованому симуляційно-емуляційному підходах. При використанні симуляційного підходу наявні певні обмеження при вивченні відповідних тематик, оскільки набір інструментів для моделювання, як правило, формується виробником і не може розширюватися. При використанні емуляційного та симуляційно-емуляційного підходів існує можливість доповнювати запропоновані виробником засоби додатковими інструментами, які підвищують ефективність процесу закріплення теоретичних знань відповідними практичними навичками.

Серед симуляційних середовищ моделювання мереж на ринку найбільш відомими є Cisco Packet Tracer, Boson Netsim, Net Cracker. Використання Cisco Packet Tracer вимагає спеціальних умов – студенти повинні бути членами мережної академії, яка створюється за спеціальною складною схемою. Boson Netsim та Net Cracker є платними і досить високовартісними продуктами. На ринку емуляційних середовищ моделювання мереж наявні як відкриті вільнодоступні розробки (наприклад, Virtual Box, GNS3), так і фірмові розробки компаній виробників мережного обладнання (наприклад, розробки фірми VMWare – VMware Workstation, VMware Server, VMware ESX Server, VMware VirtualCenter, VMware ACE, VMware Player; розробка фірми Huawei – eNSP, Enterprise Network Simulation Platform; сумісна розробка фірм HP та H3C – H3C Cloud Lab). Частина з них (зокрема, eNSP та H3C Cloud Lab) є вільнодоступними. Як правило засобів окремого емуляційного середовища недостатньо для повноцінного дослідження і вивчення роботи процесів, які відбуваються у мережі, тому їх доводиться доповнювати додатковим інструментарієм: віртуальними машинами кінцевих вузлів (як серверів, так і клієнтів на базі різних ОС), програмами аналізаторами мережного трафіку (наприклад, Wireshark, SolarWinds Response Time Viewer) тощо.

Одним з найбільш цікавих з точки зору дослідження вразливостей, мережних атак та засобів захисту є протокол DHCP. Цей протокол призначений для динамічного управління параметрами адресації кінцевих вузлів на базі клієнт-серверного підходу. Розуміння принципів функціонування даного протоколу і отримання практичних навичок з налагодження та захисту його сервісів значно підвищує рівень кваліфікації фахівця.

Очевидно, що головною ціллю зловмисника є серверна складова DHCP. Вплив на клієнтів DHCP можливий після атаки на сервер. Як відомо, архітектура протоколу дає змогу реалізувати наступні атаки на DHCP-сервер: DHCP Starvation/DHCP Exhaustion (виснаження DHCP-набору адрес); DHCP DoS (відмова в обслуговуванні DHCP); DHCP Server Spoofing/Rogue DHCP Server (фальшивий DHCP-сервер); DHCP Release (фальшиве інформування сервера про звільнення IP-адреси вузлом).

Найвідомішими засобами атак на DHCP-сервер є програмні продукти Gobbler та Yersinia. На жаль вони мають реалізацію лише для ОС Unix/Linux. Більше того Gobbler доступний не у вигляді готового рішення, а у вигляді програмного коду, тому для компіляції і використання Gobbler у системі необхідно встановити відповідні бібліотеки. Інтерфейс Gobbler – командний рядок. Yersinia є більш доступним інструментом і входить до відомого проекту Kali Linux, який доступний у вигляді віртуальної машини. Інтерфейс Yersinia має як графічну реалізацію, так і реалізацію у вигляді командного рядка. Графічний варіант Yersinia має ряд недоліків, пов'язаних із незавершеною функціональністю продукту та з не виявленими і не виправленими у процесі тестування роботи програми помилками. Командний рядок Yersinia є досить складним для застосування, вимагає значних затрат часу для формування та реалізації атак. Окрім того, розвиток проекту зупинено майже 10 років тому. Для розуміння можливостей Gobbler та Yersinia було проведене дослідження їх функціональності, яке дало можливість зробити наступні висновки: дані засоби дають змогу досить легко проводити окремі прості атаки на DHCP-сервер; організація комплексної атаки з використанням даних засобів є дуже складним процесом, вимагає значних часових затрат і не завжди призводить до кінцевого результату через внутрішні програмні помилки.

Тому було прийнято рішення розробити свій програмний продукт, який надаватиме можливість емулювати комплексні атаки на DHCP-сервер мережі Ethernet. Базовим сценарієм для комплексної атаки було визначено сценарій, який складається з наступних етапів:

Етап I. Визначення загальних параметрів адресації мережного рівня мережі.

Етап II. Сканування мережі для визначення активних вузлів та визначення фізичних (MAC-адрес) і логічних (IP-адрес) адрес вузлів.

Етап III. Виконання атаки DHCP Release від імені активних вузлів для очищення DHCP-пулу на сервері (на базі даних етапу II).

Етап IV. Виконання атаки DHCP Starvation/DHCP Exhaustion для повного виснаження DHCP-пулу на сервері (на базі даних етапу I).

Етап V. Виконання атаки DHCP Server Spoofing/Rogue DHCP Server для надання фальшивих параметрів адресації кінцевим вузлам.

Результатом реалізації базового сценарію є захоплення управління процесом динамічної адресації вузлів мережі, яке полягає у наданні кінцевим вузлам фальшивих параметрів адресації та створенні передумов для перехоплення трафіку між кінцевими вузлами та зовнішніми і внутрішніми серверами.

На основі базового сценарію було сформовано загальні вимоги до програмного продукту, розроблена загальна модель емулятора, спроектовані його внутрішня структура та інтерфейс користувача. При проектуванні враховувалася необхідність формування інших сценаріїв комплексних атак у майбутньому. Як засіб для програмної реалізації обрано середовище Visual Studio, мову C# та бібліотеки SharpPcap. Тестування виконання окремих атак, як складових комплексної атаки, та комплексної атаки в цілому здійснювалося у середовищах моделювання GNS3, eNSP, H3C Cloud Lab при умовах використання як DHCP-серверів маршрутизаторів різних виробників. Також тестування було проведено в умовах реальної мережі. Результати тестування показали 100% ефективність комплексної атаки, реалізованої за базовим сценарієм, – легітимний сервер повністю виходив з ладу, фальшивий сервер керував процесом видачі параметрів адресації кінцевим вузлам.

У подальшому планується розробка сценаріїв та компонентів емулятора, які будуть орієнтовані на обхід штатних засобів захисту від атак на DHCP-сервер, додавання можливості реалізації атак у Wi-Fi мережах, створення кросплатформенної версії емулятора атак.

Список літератури

1. Eric Vyncke, Christopher Paggen. LAN Switch Security: What Hackers Know About Your Switches. – Cisco Press, 2007. – 340 p.

2. Keith Barker, Scott Morris. CCNA Security 640-554. Official Cert Guide. – Cisco Press, 2013. – 740 p.

3. Sean Wilkins, Franklin H. Smith III. CCNP Security. SECURE 642-637. Official Cert Guide. – Cisco Press, 2011. – 738 p.

УДК 004.77:004.056

Аналіз загроз інформаційній безпеці дітей в мережі Інтернет

Задорожна Х.О., студент 4 курсу, xrustka95@mail.ru,
Кухарська Н.П., доцент, к.ф.-м.н., доцент
Львівський державний університет безпеки життєдіяльності, м. Львів

Кількість користувачів сучасних засобів масових комунікацій (насамперед, смартфонів і планшетних комп'ютерів) щодня невпинно зростає. Такі пристрої комунікації забезпечують швидкий вільний доступ до актуальної та необхідної інформації інформаційно-телекомунікаційної мережі Інтернет, сприяють підвищенню рівня ерудиції та формуванню сучасних навичок спілкування. У той же час, їх користувачі зіштовхуються з цілим спектром специфічних ризиків. Особливу небезпеку таїть в собі безконтрольний інформаційний простір для дітей – повноцінних учасників глобального інформаційного процесу. Дорослішання, навчання і соціалізація сучасних дітей проходить в умовах гіперінформаційного суспільства. І діти, як найбільш активна й допитлива аудиторія, як правило, першими опановують нові технології, часто випереджуючи в технічній освіченості батьків. Водночас, online-середовище мережі Інтернет, яка переобтяжена всім хорошим і поганим, що накопичило людство за час свого існування, може містити інформацію агресивного чи соціально небезпечного змісту. А надання дітьми переваги віртуальному світу перед реальним має дестабілізуючий вплив на їх психічний розвиток, здоров'я і психологічне благополуччя.

Чим більше часу дитина проводить за комп'ютером, тим швидше у неї виникає комп'ютерна залежність. Контент, дизайн і програмна "начинка" сайтів спеціально орієнтовані на те, щоб заманити і втримати користувачів. До комп'ютерної залежності більш схильні підлітки 14-16 років. Проаналізувавши результати наукових досліджень, присвячені вивченню феномену комп'ютерної залежності, виокремимо три основні, найбільш часті "симптоми", на які вказують вчені. По-перше, синдром "позбавлення" (відсутність доступу до Інтернету викликає негативні емоції або навіть фізичні симптоми – головний біль, безсоння). Недарма серед інтернет-користувачів гуляє популярна фраза: "Реальність – це галюцинація, викликана відсутністю Інтернету". По-друге, втрата контролю за часом і своєю поведінкою. Тут дається взнаки відома психологічна закономірність: чим більше людина поглинута змістом якоїсь діяльності, тим нижча її точність в оцінюванні часових інтервалів. По-третє, заміна реальності (надмірна важливість Інтернету у порівняні з іншими сферами діяльності). У мережі Інтернет немає минулого і майбутнього: віртуальна реальність занурює користувача у безперервне теперішнє, відірване від ритмів повсякденного життя.

Ще однією Інтернет-загрозою для дітей є доступ до небажаного контенту. Під небажаним контентом ми розуміємо матеріали, зміст яких є непридатний та/або протизаконний для дітей (такий, що пропагує культ насилля та жорстокості щодо людей і тварин, порнографію, екстремістську діяльність, вживання наркотичних засобів, психотропних і (або) одурманюючих речовин, тютюнових виробів, алкогольної продукції, тероризм, ксенофобію, сектантство, національну, класову, соціальну нетерпимість і нерівність, асоціальну поведінку, агресію, суїцид, азартні ігри, інтернет-шахрайство), перегляд яких перешкоджає позитивній соціалізації та індивідуалізації, оптимальному соціальному, особистісному, пізнавальному і фізичному розвиткові дитини, збереженню її психічного і психологічного здоров'я та благополуччя, формуванню позитивного світосприйняття.

Серед дітей і підлітків, котрі в першу чергу стають жертвами небажаного контенту, виокремимо такі групи ризику: бунтарі; самотні, такі, що відчувають труднощі у реальному спілкуванні; допитливі, ті, що прагнуть попробувати все нове, пов'язане з гострими відчуттями; довірливі, ті, які активно шукають уваги і прихильності; новачки в Інтернеті, незнайомі з мережевим етикетом; схильні до залежності; ті, які мають проблеми з сексуальною орієнтацією.

Діти залишають у мережі Інтернет цифрові "сліди" (інформацію про себе із рубрики "паспортні дані"), за якими їх можна знайти у реальному житті. 39 % підлітків викладає у мережу своє прізвище, 38 % – точний вік. Майже шоста частина підлітків готова поділитися номером свого мобільного телефону і майже стільки ж повідомити номер школи. А це вже ті відомості, за допомогою яких можна довідатися й іншу конфіденційну інформацію про дитину і її сім'ю, наприклад домашню адресу, рівень благополуччя та ін. Більше того, 1 % підлітків сам готовий повідомити незнайомцям свою домашню адресу в Інтернеті [1].

Ще одна популярна тенденція останнього часу – геотеги – географічні координати місця розташування людини чи зображеного на світлині об'єкта. Геотеги встановлюють для того, щоб поділитися з рідними чи друзями тим, що відбувається у режимі реального часу. Отримати індекси місць проживання більшості дітей нескладно. Велика кількість світлин, на яких зображені діти, мають геомітки, причому останні моделі смартфонів ставлять їх автоматично у момент знімання фотографії чи запису відео.

Кібербулінг (англ. cyberbullying від bully – хуліган, забіяка, грубіян, ґвалтівник) – електронна форма традиційного переслідування повідомленнями, що містять образи, агресію, залякування; хуліганство; соціальне бойкотування. Кіберпереслідування завдяки особливостям онлайн-спілкування стрімко поширюється у всьому світі. Оскільки електронні засоби комунікації доступні 24 години на добу, 7 днів на тиждень, жертву можна наздогнати у будь-який час і в будь-якому місці. Крім швидкості, всюдисущості, Інтернет дає змогу підхопити і ретранслювати інформацію. Інформація, яка появилася лише один раз, виходить з під контролю – образи, приниження, чутки, критика, зображення чи фотографії здатні циркулювати безмежно і нескінченно довго. Звідси наслідки для жертви – від втрати самооцінки, зниження результатів у навчанні до розвитку тривожності, а від депресивного стану – до хронічної депресії, а іноді – і до суїциду.

Зловмисники під різними приводами змушують дітей у мережі Інтернет підключатися до платних послуг. Наприклад, відіславши SMS, можна отримати доступ до закритого змісту сайту або перейти на вищий рівень в онлайн-грі. На жаль, діти не завжди помічають підступ і не звертаються за допомогою до дорослих. Як показують дослідження, 14% дітей відправляють платні SMS, і тільки деякі з них цікавляться вартістю послуги [2].

У користувачів мережі Інтернет є велика імовірність заразити комп'ютер вірусами. Сайти, пропонуючи широкий набір сервісів, як ігрових, так і для завантаження інформації різноманітної форми та змісту – фотографій, музики, відео, неявно піддають загрозі комп'ютер їх користувачів, так як ті можуть, під виглядом додатку скачати вірус чи троянську програму. Зацікавившись змістом листа від друга, дитина, не задумуючись, вибере посилання, яке може привести її на сайт, що завантажує на комп'ютер шкідливі програми.

Древньогрецький філософ Анахарсіс колись сказав, що найбільш безпечні кораблі – це кораблі, витягнуті на сушу. В Інтернеті, як в океані, немає універсального способу уникнути ризиків та загроз. Відсутність медіаграмотності і компетентності в питаннях використання інформаційних технологій у більшості випадків є основною причиною підвищеної інформаційної небезпеки. Спільні зусилля сім'ї (основного інституту соціалізації і виховання дітей), громадських організацій і держави повинні бути скеровані на вироблення у дітей навичок безпечного існування у сучасному інформаційному просторі: самостійного критичного оцінювання контенту, вміння аналізувати і відрізняти правдиві новини від дезінформації, протистояти маніпулюванню та шкідливій рекламі асоціальної поведінки. Тільки тісне співробітництво усіх учасників медіаіндустрії дасть змогу побудувати ефективну систему регулювання споживанням інформаційної продукції, максимально безпечну для здоров'я, психічного і фізичного розвитку підростаючого покоління.

Список літератури

1. Солдатова Г. Минусы открытости / Солдатова Г., Олькина О. // Дети в информационном обществе. – 2015. – № 20. – С. 36-48.

2. Кухарська Н.П. Загрози безпеці дітей у соціальних мережах // Кухарська Н.П., Кухарський В.М. // Безпека інформації. – 2014. – Т. 20, № 2. – С. 169-175.

УДК 004.056

Реалізація підсистеми інформаційної безпеки будівельної компанії

Кавун С.В., д.е.н., к.т.н., доц., kavserg@gmail.com
Харківський навчально-науковий інститут ДВНЗ УБС, м. Харків
Міхєєв І.А., к.т.н., i.a.mikheev@gmail.com
Харківський національний університет будівництва та архітектури, м. Харків

Будівництво – потужний сектор економіки, який підтримує інвестиційну активність в країні, забезпечує створення основних фондів, робочих місць різноманітної кваліфікації, впровадження інноваційних та наукоємних технологій. Як у більшості інших галузей, будівництво тісно пов'язано з інформаційною підтримкою, а отже вимагає організацію та підтримку комплексної системи інформаційної безпеки будівельних компаній та підприємств.

Інформаційну архітектуру будівельної організації пропонується розглядати на наступних рівнях:

- Організаційний рівень;
- Фізичний (апаратно-програмний) рівень;
- Рівень операційних систем і системних додатків;
- Рівень бізнес-додатків.

Забезпечення захисту кожного з рівнів інформаційної архітектури будівельної компанії, зазвичай здійснюється в рамках наступних підсистем комплексної системи інформаційної безпеки:

- управління доступом (розробка правил і політик безпеки, визначення атрибутів та регламентів доступу, організація управлінням доступом);
- забезпечення цілісності (забезпечення цілісності програмних засобів та інформації, забезпечення фізичної цілісності апаратних засобів);
- реєстрації та обліку (реєстрація будь яких: успішних і неуспішних спроб авторизування, реєстрація додавання, модифікація та видалення змін в кожну з підсистем інформаційної безпеки);
- антивірусного та мережного захисту (моніторинг антивірусної активності, забезпечення внутрішнього та зовнішнього мережевого захисту, особлива увага приділяється системам, що забезпечують роботу серверів та комунікаційних засобів);
- резервного копіювання та архівування (резервування апаратного, програмного та інформаційного забезпечення, розробка регламентів архівування інформації та даних);
- виявлення атак (контроль порушень інформаційної безпеки на усіх рівнях архітектури організації, оперативне реагування та впровадження відповідних заходів протидії на виявлені атаки);
- управління інформаційною безпекою, централізованого моніторингу та аудиту подій (реалізація функцій контролю та управління комплексною системою інформаційної безпеки, моніторинг та аналіз подій, що пов'язані з порушенням інформаційної безпеки, розробка регламентів роботи кожної підсистеми забезпечення інформаційної безпеки, періодичне звітування щодо впровадження та оцінки ефективності засобів забезпечення інформаційної безпеки).

Для кожної з підсистеми комплексної системи інформаційної безпеки можна визначити множину вимог, яким повинні відповідати певні компоненти захисту, що можуть уявляти собою комплекс організаційних заходів, спеціальних апаратних та програмних засобів. При розробці вимог до підсистеми інформаційної безпеки, її проектування і подальшій реалізації необхідно враховувати, які рівні інформаційної архітектури організації повинна забезпечувати ця підсистема.

УДК 004.108.200

Захист персональних даних в умовах розвитку інформаційного суспільства

Кавун С.В. д.е.н., к.т.н., Ph.D., доцент,
Пугачова В.І., студентка 2 курсу
Харківський навчально-науковий інститут ДВНЗ УБС, м. Харків

Сучасні суспільні відносини характеризуються широким використанням персональних даних під час обігу інформації, товарів, послуг і капіталів, що вимагає не тільки вільного руху інформації про особу, а й забезпечення її надійного захисту відповідно до основних прав і свобод людини. Прогрес у галузі інформаційних технологій, зокрема у сфері розробки та впровадження програмного забезпечення, активність у формуванні баз персональних даних надзвичайно загострили проблему захисту приватного життя фізичних осіб та захисту інших основних прав і свобод людини, саме тому зараз це є актуальною темою.

Шлях сучасного розвитку економіки країни починається з подолання деіндустріалізації та продовжується неоіндустріалізацією, у процесі якої відбувається формування інформаційного суспільства (ІС)[1]. У нашій країні цей процес розпочато, але вже давно настав час подбати про його прискорення. Застосування нових інформаційних технологій у всіх сферах життя суспільства стає характерною ознакою сучасного світового розвитку. Тому процес інформатизації, його передумови та наслідки, вплив на конкурентоспроможність економіки окремих країн оцінюють різні організації та інститути, як наприклад, Всесвітній Економічний Форум, Всесвітній банк, INSEAD Business School у співпраці з AlcatelLucent, компанія Booz, Конференція індійської промисловості та Всесвітня організація інтелектуальної власності (спеціалізована установа ООН), Організація Об'єднаних Націй. Інформаційне суспільство – це суспільство, що має розвинуту індустрію інформаційних технологій, високий рівень інформаційної культури, в якому більшість працівників зайнято виробництвом, збереженням, опрацюванням і реалізацією, особливо вищої форми-знань.

Проблемам розвитку ІС в Україні відведено важливу роль у працях багатьох науковців: О. Білоруса, В. Дергачової, Т. Шеремет (досліджено вплив на міжнародну конкурентоспроможність країни процесу інформатизації та розвитку ІС) Д. Дубова, М. Ожеван, С. Гнатюка, О. Михайловської (розкрито сучасне розуміння ІС, проаналізовано позиції України у світових рейтингах розвитку ІС). Для більшості країн розвиток інформатизації, інформаційного суспільства є одним з національних пріоритетів і розглядається як загальнонаціональна задача. Інформаційно-комунікаційним технологіям відводиться роль підґрунтя соціально-економічного прогресу, одного з ключових чинників інноваційного розвитку економіки. Україна не є виключенням цього загального процесу, підтвердженням чого є прийняті в останні роки вкрай важливі системоутворюючі нормативно-правові акти в цій сфері. Так, Законом України «Про основні засади розбудови інформаційного суспільства в Україні на 2007-2015 роки» одним з головних пріоритетів України визначено прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя. Наприклад, конвенція № 108 Ради Європи передбачає дуже важливий момент, згідно з яким збирання, накопичення, зберігання і поширення персональних даних може здійснюватися лише з дозволу особи, дані про яку обробляються. Цій особі надано право знати місце роботи та проживання розпорядника бази персональних даних (відповідального за обробку даних), а також право отримувати відповідні дані без затримки та в зрозумілій формі. У разі відмови зацікавлена особа може звернутися до суб'єкта нагляду за дотриманням законодавства в державі, який мусить забезпечити припинення порушень положень, що зазначені в національному законодавстві (ст. 8 та 13). Державна політика з реалізації цього закону знайшла своє відображення, у тому числі, в низці законодавчих актів, прийнятих протягом звітного періоду: закони України «Про доступ до

публічної інформації», нова редакція Закону України «Про інформацію», «Про захист персональних даних»[3], «Про адміністративні послуги»; Концепція розвитку електронного урядування, міжнародна ініціатива «Партнерство «Відкритий уряд» та Національна програма інформатизації. У контексті євроінтеграції України актуальною є проблема вивчення досвіду становлення ІС у країнах-членах ЄС, а також узгодження норм правових актів ЄС й інформаційного законодавства України. В Україні на найближчу перспективу необхідно: затвердити розроблену оновлену концепцію державної інформаційної політики України; у новій загальнодержавній програмі розвитку ІС в Україні на 2016-2020 рр. треба визначити пріоритети розвитку в умовах інформаційної глобалізації та євроінтеграції України; гармонізувати національну систему індикаторів розвитку ІС із відповідними показниками ЄС; адаптувати національний стандарт комп'ютерної грамотності.

Отже, відповідно до стратегії формування сучасної інформаційної інфраструктури ІС необхідно: активізувати впровадження інфраструктури широкосмугового доступу до Інтернету на всій території країни з метою розвитку Інтернету в Україні [2]; створити умови в усіх населених пунктах для доступу до Інтернету, в тому числі шляхом розбудови мережі пунктів колективного доступу; забезпечити надання всіх видів соціальної допомоги в межах єдиного державного порталу; активізувати впровадження систем електронних розрахунків за придбані товари, виконані роботи та надані послуги; поширити впровадження інтелектуальних інформаційних та інформаційно-аналітичних технологій, інтегрованих систем баз даних та знань, національних інформаційних ресурсів.

Список літератури

1. Васильєва Н.Ф. Інформаційне суспільство в Україні у світових рейтингах: стан та проблеми [Електронний ресурс] / Васильєва Н.Ф., Кавура В. Л.// Економіка промисловості. – 2015,. – №3 (71) – С. 31-43. . – Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/88605/3-Vasileva.pdf

2. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство [Електронний ресурс] / Обуховська Т.І.// Вісник НАДУ. – 2014,. – №1 – С. 95-103. – Режим доступу: http://visnyk.academy.gov.ua/wp-content/uploads/2014/05/2014-1-17.pdf

3. Конституція України. Закон України «Про захист персональних даних», № 34.

УДК 004.056

Роль сект в інформаційно-психологічній боротьбі, класифікація та ознаки сект

Константинова Л.В., викладач, liliyashel1976@gmail.com
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Інформаційно-психологічна боротьба велась у всіх протистояннях та війнах в історії. Інформаційні війни в своїй основі мають маніпулятивний вплив на масову свідомість. Вони використовують пропаганду, яка заснована на використанні особливостей людської психіки. У галузі духовного світу використовується неправда, наклеп, агітація людей, спрямована на зміну політичного ладу, вплив на сферу теоретичної свідомості (ідеологію, політичні концепції, певні соціальні принципи) і на сферу повсякденної свідомості [1]. В останні часи збільшилась активність організацій, що не є урядовими, також залучених до потрібного психологічного впливу, що сприяє потрібним політико-ідеологічним умовам у державі, на яку здійснюється вплив. Необхідно знати критерії, за якими можливо відрізняти справжню духовність від помилкової небезпечної, щоб запобігти згубного впливу.

В наш час існує широкий вибір різних духовних вчень і практик від католицизму до вчень найодіозніших та бузувірських сект, які нав'язують чужі для нашого народу культи, віровчення, навіть протиправним шляхом з використанням методик та технологій нейропсихічного програмування, гіпнозу, із застосуванням наркотичних і психотропних речовин, які пригнічують волю людини [4].

Секти і культи, що діють сьогодні можна класифікувати наступним чином:

1. Релігійні рухи, які є відносно традиційними для України - баптисти, адвентисти, лютерани, п'ятидесятники. Сьогодні ці конфесії зайняті активною прозелітичною діяльністю серед православних.

2. Секти, що мають тоталітарний характер, псевдо християнської орієнтації, такі як "Церква Христа", "Новоапостольська церква", харизматичні рухи та ін. Хоча вони і використовують Біблію як основне джерело свого віровчення, проте справжня історія секти від адептів часто і зовсім не відома.

3. Секти, які вважають себе претендентами на володіння "новим одкровенням" - мормони, "Свідки Ієгови", Біле братство та ін.

4. Вчення і секти з руху New Age, що мають окультний характер, займаються розвитком в людині надзвичайних здібностей, цілителі і чаклуни, східні культи - кришнаїзм, практики йоги, трансцендентальна медитація, астрологія, валеологія та ін.

5. Сатанинські культи, що відрізняються жорстокістю і спираються переважно на молодь. Туди потрапляють через юнацький нігілізм, заперечення авторитету батьків, суспільства, Бога, спрагу безкарності. Вербування відбувається на різних молодіжних заходах, найчастіше рок-концертах. Молодь залучають окультними фокусами, наркотиками, статевою розпустою, культом насильства. Моральність відхиляється, аморальність стає нормою, сила і безжалісність – звеличуються [2].

За деякими ознаками можна розпізнати секти:

1. Секти поширюють своє вчення і здійснюють вербування нових членів особливими засобами.

2. Сектам притаманний агресивний прозелітизм та психологічний тиск.

3. Вербувальники сект не повідомляють тим, кого намагаються залучити в секту, всієї правди про історію секти, її засновника і її справжнє віровчення тому, що в сектах є подвійне вчення - одне для реклами своєї секти, а інше - для внутрішнього користування.

4. В секті існує певна ієрархія.

5. Вчення секти завжди претендує на те, що це найвища істина, причому істина "свіжіша", ніж істини всіх інших релігій.

6. В сектах відбувається програмування свідомості.

7. Члени секти вважаються особливими врятованими, інші – приреченими.

8. Сектантська організація намагається контролювати всі сфери життя її членів.

9. Політичні цілі. Церква Об'єднання Муна, "Свідки Ієгови", саєнтологія Рона Хаббарда та інші секти, представляють собою промислових та фінансових магнатів, маючи за мету отримати владу над світом. Наприклад, "Маніфест Варнашрама", це документ "Міжнародного товариства свідомості Крішни". В ньому зазначено, що в перспективі суспільство кришнаїзму переможе і буде розділене на касти - рабів і еліту, тобто надлюдей, що будуть вирішувати долю інших [2].

Вербувальники сект широко застосовують соціальні мережі.

Факт участі релігійних рухів у політиці не може бути оцінений негативним чи позитивним для держави та для суспільства. В одних випадках це може бути вигідно для суспільства і направлено на зміцнення держави [5]. Необхідно розрізняти невинне просте прагнення релігійної організації сформувати у людей про себе позитивну думку від спланованих цілеспрямованих ідеологічних дій сект.

Політична пропаганда проглядається у діях сект особливо в умовах політично нестабільного стану держави. Релігійна форма виступів проти соціальної несправедливості посилює та збільшує протест [5].

Деякі секти являють собою інструмент, завдяки якому можна здійснювати вплив на країну, де вони знаходяться, та нероздільно пов’язані з політикою. Члени сект відіграють велику роль, впливаючи на результат будь-яких виборів. Їх голос залежить від наказу лідерів. Навіть за активністю сектантів можна зрозуміти прихильність до того чи іншого кандидата їх лідерів.

Також секти застосовуються у якості фактору впливу у міжнародній політиці. Це може мати найрізноманітніші цілі та задачі.

Багаточисельні приклади підтверджують застосування сект різними державами світу як інструменту для проведення розвідувальної діяльності [5]. Військові впроваджувались в громади потрібної релігійної організації в різних країнах світу для того, щоб використати їх в якості засобу для прихильності та підкорення людей. Ставши пасторами добре підготовлені спеціалісти впливають на весь рух.

Одним з чинників виникнення і розвитку тероризму та релігійних війн є секти. М. Олбрайт вважає, що в ідеалі чіткий поділ релігії і політики міг би стати виходом з стану релігійної війни [6].

Висновки. Сьогодні секти народжуються з завідомо визначеними цілями – керувати свідомістю людей. У правильних обставинах слова володіють не меншою силою, ніж снайперська гвинтівка, але у наших силах протистояти інформаційним впливам, і зробити це простіше за все, вибираючи свої джерела інформації. В секти майже не потрапляють люди в результаті пошуків, керуючись роздумами, порівняннями.

Список літератури

1. Дубас О. П. Інформаційна війна: нові можливості політичного протиборства [Електронний ресурс]. – Режим доступу: http://social-science.com.ua/article/180

2. Классификация и признаки сект [Електронний ресурс]. – Режим доступу: http://forum.detective-agency.info/ru/viewtopic.php?f=82&t=2818

3. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222

4. Галамба М. Сутність, види та методи спеціальних інформаційних операцій [Електронний ресурс]. – Режим доступу: http://justinian.com.ua/article.php?id=2524

5. Мартинович В.А. Секты и политика в Беларуси. // Международная научно-практическая конференция Европейской Федерации Центров по исследованию и информированию о сектантстве (FECRIS) «Тоталитарные секты и право человека на безопасное существование». – Санкт-Петербург. 15-16 мая 2009. –С.1-10.

6. Олбрайт М. Религия и мировая политика. – М.: Альпина Бизнес букс, 2007. - 352с.

УДК 004.056.53(044)

Захист мережного трафіку на базі потокових алгоритмів RC-5 та RC-6

Корнієнко Б.Я., д.т.н., доцент, завідувач кафедри КСЗІ, bogdanko@i.ua,
Кучерка М.В., студентка 4 курсу НН ІКІТ
Національний авіаційний університет, м. Київ

Криптографія сьогодні – це найважливіша частина всіх інформаційних систем: від електронної пошти до стільникового зв'язку, від доступу до мережі Internet до електронної готівки. Використання криптографічного захисту інформації під час побудови політики безпеки банківської on-line-системи значно посилює безпеку роботи системи, але за умови, що ця система захисту створена належним чином та має безпечну систему розподілу криптографічних ключів.

Мета роботи – розробка та порівняльна характеристика алгоритмів шифрування RC5 і RC6.

Алгоритм RC5 був розроблений Рональдом Рівестом (Ronald L. Rivest) для компанії RSA Data Security. На основі RC5 свого часу був створений алгоритм шифрування RC6, який брав участь в конкурсі на звання AES (Advanced Encryption Standard - "Кращий" алгоритм шифрування), оголошеному національним інститутом стандартизації і технологій для заміни вже застарілого алгоритму DES. Тоді RC6 не виграв тільки із-за низької продуктивності апаратних реалізацій алгоритму. А програмні реалізації RC5 і RC6 є, мабуть, найшвидшими серед всіх алгоритмів шифрування, що забезпечують достатню стійкість перед атаками.

Алгоритм RC5 шифрує блоки відкритого тексту довжиною 32, 64 чи 128 бітів в блоки шифрованого тексту тієї самої довжини. Довжина ключа може змінюватись від 0 до 2040 бітів. Конкретна версія RC5 позначається RC5-w/r/b. Наприклад, RC5-32/12/16 використовує 32-бітові слова (64-бітові блоки відкритого і шифрованого тексту), 12 раундів шифрування і ключ довжиною 16 байтів (128 бітів).

RC6 — симетричний блоковий криптографічний алгоритм, похідний від алгоритму RC5. Був створений Роном Рівестом, Меттом Робшау і Реєм Сіднеєм для задоволення вимог конкурсу Advanced Encryption Standard (AES). Даний алгоритм був одним з п'яти фіналістів конкурсу, також представлений NESSIE і CRYPTREC. Він є власницьким (пропрієтарним) алгоритмом, і запатентований RSA Security.

Варіант шифру RC6, заявлений на конкурс AES, підтримує блоки довжиною 128 біт і ключі довжиною 128, 192 і 256 біт, але сам алгоритм, як і RC5, може бути налаштований для підтримки більш широкого діапазону довжин як блоків, так і ключів (від 0 до 2040 біт). RC6 дуже схожий на RC5 за своєю структурою і також досить простий у реалізації.

На відміну від багатьох інших алгоритмів шифрування RC6 не використовує довідкові таблиці під час шифрування. Це означає, код RC6 і дані можуть міститися в сучасній кеш-пам'яті і тим самим економити місце в пам'яті.

При створенні програмного забезпечення захисту інформації особливу увагу слід приділяти безпечній реалізації таких програм. Так, наприклад, основними операціями з ключами шифрування є створення, знищення та встановлення значення. З метою запобігання розповсюдження ключової інформації в інші частини програми, операція знищення має заповнити нулями область пам'яті, виділену для роботи з ключем, перед тим, як звільняти її менеджеру пам'яті.

Список літератури

1. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

2. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

УДК 621.395.7

Метод линейного целочисленного декодирования псевдослучайных кодов

Лавровская Т.В., аспирант кафедры БИСТ, lavrovska@gmail.com,
Рассомахин С.Г., д.т.н., доцент, rassomakhin@karazin.ua
ХНУ им. В.Н. Каразина, Харьков, Украина

Введение

На сегодняшний день псевдослучайное кодирование является практически единственным способом для обеспечения требуемого уровня помехозащищенности информации, циркулирующей в сети со случайными и умышленными угрозами. Теоретической основой, подтверждающей корректность данного тезиса, является работа К. Шеннона. В которой было доказано, что использование псевдослучайного кодирования в канале с помехами, позволит достичь произвольно малой вероятности ошибки, при увеличении длинны блока кода.

Практическое доказательство данного тезиса выполнено в работах [1, 2]. Построение ПСК на основе кодовых слов, которые выбираются равномерно случайно из заданного диапазона, показали, что практически любой случайный код является достаточно "хорошим". Объем полезно используемого для размещения кодовых точек евклидова пространства кода и средние взаимные расстояния с увеличением длины блока стремятся к наилучшим значениям. Такие коды обеспечивают одновременно частотную и энергетическую эффективность и могут успешно применяться при использовании многопозиционных методов амплитудно-фазовой модуляции, находящих все более широкое распространение в современных стандартах, цифровых СПИ.

Цель работы: разработка вычислительно реализуемого математического метода декодирования псевдослучайных кодов (ПСК) для безопасной передачи данных в компьютерных сетях и перспективных системах мобильной связи, на основе использования модифицированного метода ветвей и границ.

Основная часть

В рамках данной работы для генерации псевдослучайных чисел использовался линейный конгруэнтный генератор (ЛКГ). При построении блоков кода генерируемые канальные символы (числа, соответствующие значениям информативного параметра сигнала-переносчика) распределялись равномерно случайно в заданном диапазоне 2^n, где n – длина блока кодового слова. Кодовый блок ПСК $X = \{x_0, x_1, \cdots, x_{n-1}\}$ определяется порождающим числом последовательности x_0, которое, является лексикографическим номером кодируемого сообщения. На основе x_0 формируется еще $(n-1)$ символов по рекуррентному правилу:

$$x_i = \mathrm{mod}((a \cdot x_{i-1} + b), m), \text{ где } i \in [1, n-1], \quad (1)$$

где числа a, b, m – целые положительные константы, удовлетворяющие условиям: $m \geq 2^n$, b и m – взаимно простые числа, величина $(a-1)$ − кратна любому простому числу, которое меньше m и является его делителем.

Однако, алгоритм генерации последовательности является нелинейным, что не дает возможности реализовать линейные алгебраические методы декодирования с приемлемой вычислительной сложностью.

Для достижения поставленной цели, была осуществлена линеаризация задачи декодирования путем введения дополнительного параметра у:

$$x_{i+1} = a \cdot x + b - y_i m, \; i \in [0,1,...,n-2] \; . \quad (2)$$

Данное выражение является правилом алгебраической линеаризации нелинейной операции вычисления по модулю при генерации очередного $(i+1)$ символа. Выражение справедливо только в случае выполнения двустороннего ограничения:

$$0 \le y_i \le \left\lfloor \frac{(m-1)a+b}{m} \right\rfloor \quad (3)$$

где y_i – целые числа, $i \in [0, n-2]$.

Для декодирования блока ПСК доступным является наблюдение искаженного в канале произвольного j -го кодового слова $Z_j = \{z_0{}^j, z_1{}^j, \cdots z_{n-1}{}^j\}$, $Z_j = X_j + H$, где $H = \{\xi_0, \xi_1, ..., \xi_{n-1}\}$ – вектор помехи. При этом производятся формулировка и формализация канонической задачи линейного целочисленного программирования. Целый ряд формальных признаков получаемой целочисленной задачи факторизации порождающего числа x_0 предопределяют целесообразность применения для ее решения метода ветвей и границ, обладающего вычислительной сложностью не выше полиномиальной от параметра n.

Для решения линеаризованной задачи декодирования предложено применение табличного алгоритма симплекс-метода последовательного поиска оптимальных опорных планов задачи в узлах ветвления дерева решений. При этом потребовалась некоторая модификация стандартного метода поиска ближайшего к наблюдаемому кодового слова ПСК. Для корректной оценки возможного искажения каждого символа полученного кодового слова Z_j вводятся переменные двусторонней оценки отклонения числа w_i, где $i \in [1, 2n]$. Это позволяет заменить нелинейный метод поиска минимального взаимного евклидова расстояния между кодовыми словами приближенным линейным методом поиска минимальной суммы проекций разностного вектора $Z_j - X_i$, $i, j \in [0, m-1]$. При этом вводимые компенсационные переменные объединяются в пары $(w_1, w_2), \cdots, (w_{2n-1}, w_{2n})$, причем переменные с нечетными и четными номерами используются в уравнениях-ограничениях задачи с противоположными знаками, характеризуя тем самым возможные двусторонние отклонения символов (чисел) кодового слова. В полной записи формализованной задачи фигурирует $3n-1$ уравнений-ограничений, содержащих $5n-1$ неизвестных. Таким образом, как минимум, $2n$ переменных в начале решения задачи имеют статус свободных.

Цель работы достигается за счет того, что поиск минимума осуществляется для линейной целевой функции вида:

$$L = \sum_{i=1}^{2n} w_i = w_i + w_{i+1} + ... + w_{2n} \quad (4)$$

Статистические исследования предложенного метода декодирования доказывают достижение поставленной цели – обеспечение вычислительной сложности процесса декодирования ПСК не выше полиномиальной.

Выводы:

Рассмотренный метод декодирования ПСК незначительно проигрывает по объективности методам, основанным на ПМП, однако имеет возможность компенсировать данный недостаток путем увеличения длинны блока до практически требуемых значений. Применение ПСК в сочетании с разработанным методом декодирования позволяет практически использовать ПСК в современных высокоскоростных СПИ.

Литература:

1. Лавровская, Т.В. Анализ применения правила простого округления для получения вычислительно реализуемых методов декодирования / С.Г. Рассомахин, Т.В. Лавровская // Системи обробки інформації. – 2015. – вип. 5 (151). – с. 115-117.
2. Лавровская, Т.В. Оценка эффективности псевдослучайных кодов, сгенерированных с помощью LFSR / С.Г. Рассомахин, Т.В. Лавровская, О.И. Вотяков // Прикладная радиоэлектроника. – 2016. – том. 14/ вып. 4. – с. (в печати).

УДК 004.057.4

Дослідження методів криптоаналізу сучасних криптографічних алгоритмів

Лагун А.Е., к.т.н., доцент, a.e.lagun@gmail.com,
Кухарська Н.П., к.ф.-м.н., доцент, kukharska.n@gmail.com
Львівський державний університет безпеки життєдіяльності, м. Львів

На цей час, через бурхливий розвиток комп'ютерної техніки і відкритих мереж, сучасних методів передавання та обробки інформації, з'явилися нові види загроз і вразливостей, пов'язані з можливістю втрати, розкриття, модифікації даних, що належать різним користувачам. Для забезпечення захисту інформації в комп'ютерних системах актуальним є дослідження та вдосконалення криптографічних алгоритмів, що убезпечують користувачів від інформаційних загроз.

Визначення ефективності криптографічних алгоритмів, як правило, є складнішою задачею, ніж його проектування, оскільки воно вимагає більших знань і тому є більше науковою, ніж інженерною задачею. Це призводить до того, що існує велика кількість засобів криптографічного захисту, надійність яких не є визначеною та гарантованою, оскільки алгоритми, на яких вони базуються, є мало дослідженими.

Атаки на криптографічні алгоритми

Основною метою атаки на алгоритм шифрування є знаходження відкритого тексту за допомогою відомого шифротексту і невідомого ключа шифрування або безпосередньо пошук ключа шифрування для можливості розшифрування зашифрованих цим ключем повідомлень. Тому актуальним є проведення досліджень методів криптоаналізу для оцінки стійкості існуючих криптографічних алгоритмів. Класифікацію сучасних методів криптоаналізу наведено на рис. 1.

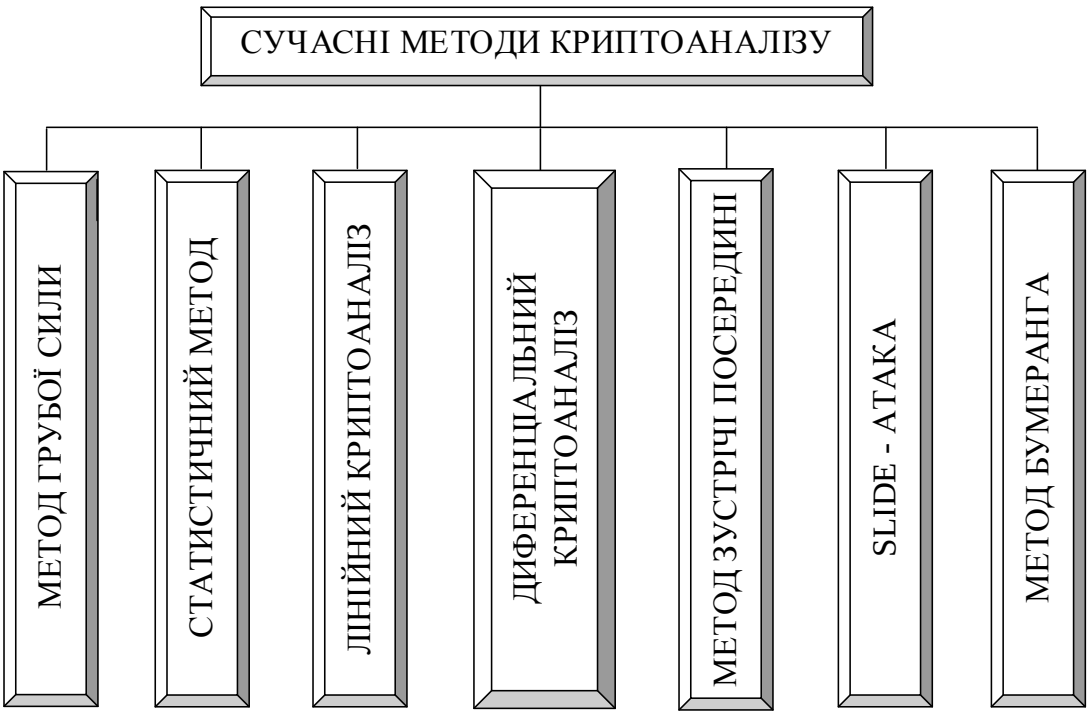


Рисунок 1 – Класифікація сучасних методів криптоаналізу

При використанні методу грубої сили відбувається перебір всіх можливих варіантів ключа шифрування, в результаті чого ключ шифрування буде обов’язково знайдено. Наприклад, якщо потрібно знайти ключ довжиною k біт, то такий пошук вимагатиме 2^{k-1} тестових операцій шифрування. Захистом від атак методом грубої сили є збільшення величини ключа, оскільки при

збільшенні величини ключа на один біт кількість комбінацій ключа шифрування збільшується в два рази.

Зрозуміло, що навіть при сучасному розвитку обчислювальної техніки, метод грубої сили не є ефективним, проте його можна покращити при використанні спеціальних пристроїв перебору або розпаралелюванні процесу пошуку ключів.

При використанні статистичного аналізу потрібно визначити ключ шифрування або його частину, маючи деяку кількість пар "відкритий текст – шифротекст". Основою статистичного аналізу є процедура статистичної класифікації, яка для великої кількості статистичних даних, що вибираються випадковим чином, визначає закон розподілу цих даних і шуканий параметр – ключ шифрування.

Лінійний криптоаналіз поєднує пошук лінійних статистичних аналогів для рівнянь шифрування, статистичний аналіз відкритого та шифротексту, а також методи узгодження та перебору. Даний метод досліджує статистичні лінійні залежності між окремими бітами масивів відкритого, шифротексту та ключа і використовує ці залежності для визначення статистичними методами окремих біт ключа.

У методі лінійного криптоаналізу формуються залежності між відкритим текстом, шифротекстом та ключем. Ці залежності повинні мати високу ймовірність і разом з відомими парами "відкритий текст – шифротекст" використовуються для отримання бітів ключа. Для захисту від атак з використанням лінійного криптоаналізу необхідно досягти того, щоб при будь-якій зміні відкритого тексту або ключа кожен з бітів шифротексту змінювався з різною ймовірністю.

У диференціальному криптоаналізі використовуються пари шифротексту, що мають деяку відмінність. У процесі аналізу досліджуються властивості даної відмінності при шифруванні відкритих текстів одним ключем. Зокрема, вибираються два відкритих тексти з фіксованою відмінністю і після процесу шифрування аналізується відмінність в отриманих шифротекстах. Потім різним ключам присвоюються різні ймовірності. В процесі подальшого аналізу наступних пар один з ключів стане більш ймовірним, тому він і є ключем шифрування.

Існує також посилений варіант диференціального криптоаналізу, який використовує не два, а чотири відкритих тексти та відповідних їм шифротексти, що пов'язані певною структурою, і називається методом бумеранга. Цей метод важко застосувати на практиці.

Метод зустрічі посередині використовує ідею парадоксу днів народження, яка полягає в тому, що для $x\sqrt{y}$ ключів, вибраних з множини y, ймовірність їх збігу дорівнює $(1 - exp(x^2/2))$. Пошук ключа шифрування зводиться до пошуку еквівалентної йому пари. Алгоритм працює так. На першому етапі для відкритого тексту фіксують ключ шифрування і одержаний шифротекст. На другому етапі випадковим чином вибирають ключ розшифрування довільного шифротексту. У випадку збігу шифротекстів і відкритих текстів з першого і другого етапів ключі шифрування з цих етапів будуть шуканим ключем, інакше етапи пошуку повторюють.

Висновки. Розглянуті методи криптоаналізу дають змогу виявити недоліки і слабі місця різних криптографічних алгоритмів, врахувавши які можна підвищити стійкість сучасних криптосистем.

Список літератури

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. – М. : Триумф, 2002.

2. Ковтун В. Ю. Введение в криптоанализ. Криптоанализ симетричных криптосистем: блочные шифры. – Санкт-Петербург, «БХВ-Петербург», 2009.

3. Andriy Lagun Cryptographic Strength of a New Symmetric Block Cipher Based on Feistel Network // Technical Transactions. Series "Automatic Control". – 2013. – Vol. 2-AC (10). – P. 67-80.

УДК 621.373

Пасивні засоби захисту від лазерних систем акустичної розвідки

Малишев Р.А., студент 4 курсу, malyshevroman.a@gmail.com
Науковій керівник – к. т. н., проф. Заболотний В. І.
Харківський національній університет радіоелектроніки, м. Харків

«*Якщо не впевнений у безпеці, вважай, що небезпека існує реально*» (Правила морського судноплавства).

На сьогоднішній день системи захисту покращуються, ускладнюються і стають більш універсальними. За законами природи як тільки покращується система захисту – одразу ж покращується і система атаки.

Одними з найнебезпечніших електронних пристроїв перехоплення мовної інформації можна вважати засоби дальньої розвідки, адже зловмиснику не потрібно мати доступу до приміщення і він легко здатен отримати потрібну йому інформацію. До таких засобів належать спеціальні лазерні мікрофони, а канал витоку інформації з їх використанням називають оптико-електронним. Лазерний мікрофон для акустичного спостереження або пристрій для лазерного прослуховування на далеких відстанях є високотехнологічним апаратом для збору інформації, в якому використовується невидимий інфрачервоний лазерний промінь, за допомогою якого проводиться підслуховування розмов цільового об'єкта. Цей пристрій є найбільш ефективним пристроєм для віддаленого лазерного прослуховування (лазерним мікрофоном) в світі і дозволяє оператору виконувати прослуховування аудіо сигналів, яке не детектується, і виходять з будь-якого цільового приміщення, що має, принаймні, одне вікно, на значній відстані, яке становить більше 500 метрів .

Для захисту приміщення від витоків по оптико-електронному каналі застосовують як активні, так і пасивні методи захисту. Активні методи використовують генератори шуму і датчики, які здатні генерувати завади. До пасивних відносять звукоізоляцію та екранування. Одним із пасивних засобів захисту мовної інформації по оптико-електронному каналу є віконні плівки. Ці засоби являють собою полімерні плівки, вкриті з одного або з двох боків клейким розчином (адгезивом), здатним прилипати до скляної поверхні. Це багатошарові структури, що складаються з різних комбінацій прозорого поліестеру, пофарбованого поліестеру, металізованого (металізація методом електронного променя) або спатерного поліестеру (металізація методом іонного обміну в атмосфері інертного газу) й інсталяційного клею. Область використання відповідно до цілей приведені у таблиці 1.

Таблиця 1 – Сфери використання захисних плівок

Ціль	Область використання	Засоби захисту
Захист акустичної інформації від зчитування за допомогою лазерного випромінювання	Спецприміщення обладнані для переговорів; комп’ютерні зали	Скло з захисною металізованою срібною або бронзовою плівкою
Захист приміщень від перегляду ззовні сторонніми особами	Пункти охорони, внутрішні робочі приміщення та ін.	Скло з дзеркальною тонованою плівкою
Непрозорі скляні конструкції з частковим або нульовим світопропусканням	Фотолабораторії, внутрішні робочі приміщення та ін.	Скло з матовою або непрозорою плівкою

Також захисні плівки класифікують за технологією виготовлення та прозорістю – табл. 2.

Таблиця 2 – Класифікація захисних плівок за прозорістю та технологією виготовлення, Кп – коефіцієнт прозорості.

<table>
<tr><td colspan="4">Захисні плівки</td></tr>
<tr><td>Прозорі(Кл(90-95%))</td><td colspan="2">Частково прозорі(Кл(65-70%))</td><td>Малопрозорі(Кл(15-20%))</td></tr>
<tr><td></td><td>Спатерні (Технологія магнетронного або імпульсного лазерного напилювання)</td><td>Забарвлені</td><td>Металізовані (Технологія молекулярного випаровування у вакуумі)</td></tr>
</table>

Зі згаданих вище захисних плівкових технологій найактуальнішими для цілей захисту інформації слід вважати металізовані та спатерні плівки, які здатні відбивати ближнє та середнє інфрачервоне випромінювання, що можна застосувати для блокування зчитування вібрацій скла за допомогою лазерного променя, таким чином виключаючи можливість спостереження за об'єктами захисту в кабінеті, зменшують освітленість кабінету незначною мірою, але дозволяють легко виявити вікна приміщень з підвищеними вимогами до безпеки інформації, що істотно спрощує процес розвідки для зацікавленої сторони. Заклеєне плівкою вікно явно виділяється на тлі інших і тому, з міркувань скритності захисту, наносити такі плівки на вікна охоронюваного приміщення не завжди гарна ідея. Для забезпечення скритності захисту застосовувати плівку треба на всіх вікнах, принаймні, поверху, а краще будівлі.

Металізовані плівки містять шар металізованого поліестеру, ламінований шаром прозорого або пофарбованого поліестеру, а також шар захисного прозорого поліестеру відповідної товщини. Спатерні плівки виготовляються нанесенням тугоплавких металів із застосуванням методу іонного обміну в атмосфері інертного газу або методу магнетронного напилення.

Ще існує вид плівок, який використовує принцип накладання хвиль: товщина плівки підбирається таким чином, щоб вона була рівна чверті довжини хвилі. У такому разі хвиля, що відбилась від плівки, буде накладатись у протифазі на хвилю, що відбилась від скла, що забезпечить дуже надійний захист від розвідки ЛЗАР. Очевидним недоліком є необхідність знати заздалегідь параметри сигналу, яким будуть опромінювати приміщення, що захищається. Універсальної плівки для всіх довжин хвиль не існує.

Мовна інформація – неодмінний атрибут сучасної економіки, політики, сфери фінансів чи послуг. Ціна такої інформації може бути надзвичайно великою, і саме ця ціна породжує гостру необхідність у захисті даної інформації. Для вирішення цієї проблеми, на сьогоднішній день, є широкий вибір засобів, це дозволяє вибирати той, який більше задовольняє і підходить під конкретну ситуацію. Комбінуючи активні і пасивні методі можна досягти більш високого рівня захисту.

УДК 004.49

Розробка автоматизованої системи для проведення аудиту інформаційної безпеки комп'ютерних систем та мереж «Vine»

Мелешко Є.В., канд. техн. наук, доцент, elismeleshko@gmail.com
Хох В.Д., лаборант, ch2oa516@gmail.com
Кіровоградський національний технічний університет, м. Кіровоград

Аудит інформаційної безпеки (АІБ) – це системний процес одержання об'єктивних якісних і кількісних оцінок поточного стану безпеки інформаційної системи або інформаційно-телекомунікаційної системи, комплексна оцінка рівня інформаційної безпеки системи, що проходить аудит з урахуванням трьох факторів: персоналу, процесів та технологій. Порівняльний аналіз поточного стану інформаційної системи, що визначається за підсумками анкетування, з тестовою моделлю вимог стандарту ISO 27001. Аудит ІС та ІТС проводиться на відповідність вимогам [1]:

- Нормативних документів у галузі технічного захисту інформації України (НД ТЗІ).
- ISO/IEC 27001:2005 (поточна редакція 2013).
- PCI DSS.

Ціллю розроблюваної системи є часткова або повна автоматизація АІБ комп'ютерних систем та мереж, шляхом моделювання ситуації атаки на систему, що проходить аудит.

До найближчих аналогів даної системи можна віднести комплекси програмного забезпечення на зразок Armitage, який, по-суті, є графічним інтерфейсом, що об'єднує Metasploit Framework, сканер nMap та має інтегровану систему пошуку по базі експлойтів Metasploit Framework, на основі результатів сканування. Armitage не має інтегрованої експертної системи, а відтак не може генерувати певні нові рішення.

Розроблювана система відрізняється від подібних, використанням у своєму ядрі експертної системи (ЕС). Розроблена ЕС використовує апарат нечіткої логіки та продукційну модель представлення знань. Однією з особливостей розробленої системи є реалізація механізму просторів імен, що дозволяє значно пришвидшити роботу системи, а також, у деяких випадках, відновити певні данні, які були не помічені або проігноровані користувачем-оператором. Механізм простору імен споріднений з механізмом простору імен в Сі-подібних мовах програмування у тому сенсі, що простір імен визначає область видимості фактів та продукцій. Один і той же факт може бути по-різному обчислений у різних просторах імен. До того ж під час роботи експертів по заповненню або редагуванню бази знань може виникати ситуація, коли продукція використовує декілька фактів з різних просторів імен – система спроможна відтворити такі зв'язки, увімкнувши додатково певні простори імен. Так користувачу надається більше простору для творчого пошуку вирішення проблеми, а на систему лягає задача забезпечити працездатність цих рішень. Схема побудови або відновлення подібних зв'язків наведена на рис. 1.

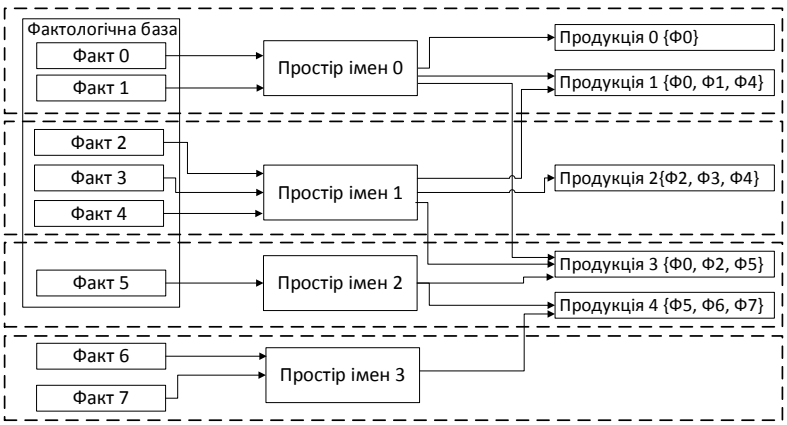


Рисунок 1 – Схема відновлення зв'язків за допомогою механізму простору імен

Один з механізмів, який дає змогу автоматизувати процес керування простором імен і зробити його більш точнішим – механізм фактів-трігерів. Факт-трігер – це такий факт, значення якого явно вказує на певний простір імен, наприклад, якщо системі доведеться проводити АІБ мережі, в якій усі пристрої використовують одну й ту ж саму операційну систему і її версію. Такий механізм значно зменшить кількість проходів по базі знань.

Роботу системи можна поділити на 2 етапи. На І етапі користувач щільно співпрацює з ЕС, намагаючись якомога точніше охарактеризувати область своїх інтересів, на цьому етапі формуються дві перші версії фактологічної бази (ФБ):

– 1 версія – формується повністю на основі вказівок користувача, йому доступна можливість додавання або виключення фактів з ФБ, вільно змінювати властивості фактів.

– 2 версія – формується із використанням механізму відновлення зв'язків за допомогою просторів імен. Система дає змогу користувачу надати додаткові данні, які їй невідомі. Користувач не може виключати факти, але може додавати або змінювати властивість факту на факт-трігер або звичайний.

На ІІ етапі система розробляє своє рішення та надає набір інструкцій, які будуть надіслані провайдеру інструментів за допомогою протоколу SSH. Вхідними даними на цьому етапі є ФБ з визначеними фактами. Вихідні дані – черга з блоками інструкцій. Черга надається як результат роботи ЕС на розсуд користувача, який сам приймає рішення, який з блоків застосувати, або модифікувати і потім застосувати. Схему роботи системи зображено на рис. 2.

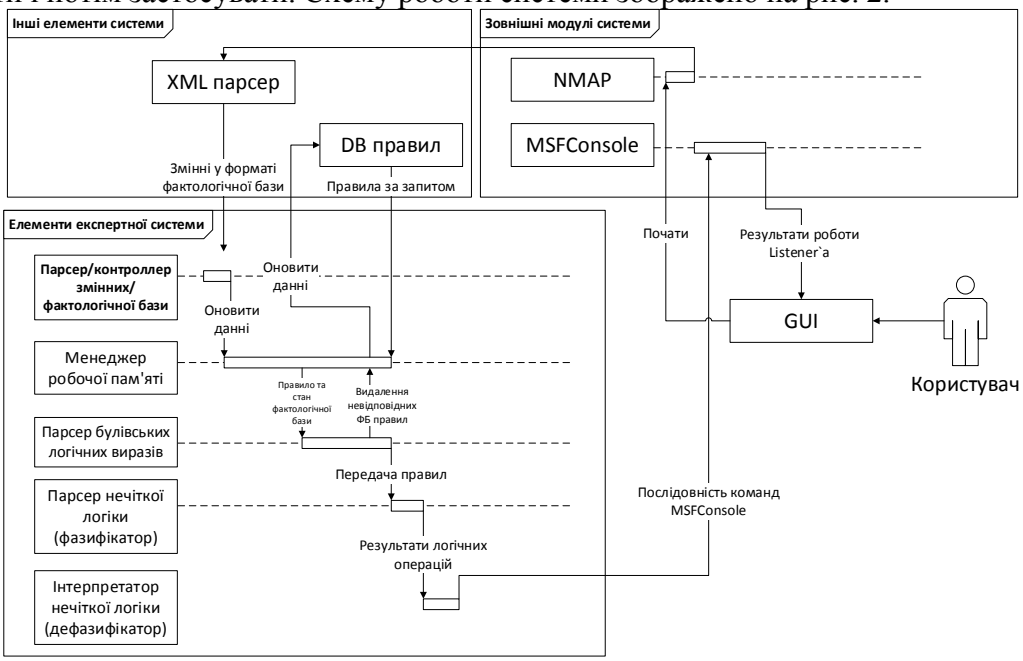


Рисунок 2 – Загальна функціональна схема системи

Розроблювана система досить гнучка, що дозволяє застосовувати її з OSSTMM (Open Source Security Methodology Manual) [3] та методологією NIST (National Institute of Standards and Technology) [4]. В наступних версіях розробленої системи планується реалізувати:

– Використання розподілених сканувань систем, що підлягають АІБ.

– Автоматизація процесів розподілених сканувань та атак за допомогою ЕС.

– Розробка протоколів ефективного розподілу навантаження серед вузлів системи.

Ефективний розподіл завдань серед вузлів планується розробляти на основі протоколів рівнорангових мереж, на кшталт протоколу Kademlia.

Список літератури

4. Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security

5. iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс]. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html

6. Open Source Security Testing Methodology Manual (OSSTMM) [Електронний ресурс]. – Режим доступу: http://www.isecom.org/research/osstmm.html

7. Technical Guide to Information Security Testing and Assessment [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

УДК 004.056.57

Спосіб організації захисту серверу гри для програмістів

Міхав В.В., студент, mihaw.wolodymyr @gmail.com
Науковий керівник – Паращук С.Д., к.ф.-м.н., доцент
Кіровоградський державний педагогічний університет ім.В.Винниченка, м. Кіровоград

Ігри для програмістів давно зайняли свою нішу на ринку. Загальновідомо, що великі IT-компанії використовують такі ігри для розв'язання складних алгоритмічних завдань. Системи для проведення олімпіад з програмування (наприклад ejudge чи Яндекс.Contest) працюють за схожими принципами. Одна з головних проблем, що виникають під час розробки таких систем – це безпечність коду користувача.

Запропоновано метод організації захисту серверу гри для програмістів на основі ізоляції потенційних небезпек.

Алгоритм запуску програми користувача на сервері гри складається з наступних етапів:

1. отримання сирцевого коду програми користувача;
2. компіляція коду (пропускається для інтерпретованих мов програмування);
3. запуск екземпляру серверної програми;
4. запуск користувацьких програм, перенаправлення потоків введення/виведення;
5. періодичне опитування сервером користувацьких програм.

Більшість систем використовує такий або подібний алгоритм дій. Але деякі системи отримують одразу відкомпільовані програми; такий підхід дозволяє уникнути розсекречення коду, проте відкриває додаткову вразливість системи.

Система захисту серверу гри полягає у максимальній ізоляції програм користувачів. Вона здійснюється за допомогою наступних дій:

1. запуск серверу гри у в'язниці за допомогою команди *chroot* (UNIX) (не підходить для ОС Windows);
2. відімкнення заголовкових файлів, що містять потенційно небезпечні функції;
3. пошук у сирцевому коді викликів функцій для роботи з іншими програмами, потоками, файловою системою та мережею. Якщо такі виклики було знайдено, запуск програми скасовується;
4. компіляція користувацьких програм безпосередньо перед запуском (захищає від заміни бінарного файлу зловмисниками);
5. обмеження максимального об'єму віртуальної пам'яті для користувацької програми за допомогою *setrlimit*() (UNIX) або робочого об'єкту (Windows);
6. встановлення обмеження на час відгуку;
7. призупинення програми користувача на час очікування відгуку від інших програм.

Переваги запропонованого способу:

- багаторівневість захисту;
- операційна система не зазнає пошкоджень навіть у випадку здійснення зловмисних дій користувацькою програмою.

До недоліків можна віднести прив'язку методу до операційної системи (можна уникнути за допомогою використання директив прекомпіляції).

Висновки. Показано проблему, яка виникає при створенні системи для автоматичної перевірки сирцевих кодів (в тому числі й ігор для програмістів чи олімпіад з програмування). Запропоновано спосіб організації захищеного середовища для таких систем на основі функцій операційної системи та контролю вмісту сирцевого коду.

УДК 004.738.5

Загрози інформаційній безпеці держави в соціальних інтернет-сервісах

Молодецька К.В., доцент, kmolodetska@gmail.com
Житомирський національний агроекологічний університет, м. Житомир

Сьогодні постійно зростає роль соціальних інтернет-сервісів (СІС) як електронної платформи для соціальної комунікації громадян [1-3]. Велика кількість сучасних СІС дозволяє учасникам взаємодії у СІС, яких називають акторами, обрати найбільш зручний і ефективний засіб поширення контенту й комунікації, реалізації особистісних та групових інтересів. Популярність СІС зумовлена широкими можливостями для спілкування, розповсюдження мультимедійного контенту різного типу, створення подій з метою перенесення віртуальної взаємодії акторів оффлайн тощо. Однак, СІС окрім усіх позитивних комунікаційних характеристик є джерелом загроз інформаційній безпеці держави (ІБД) [1, 3]. Використання віртуальних спільнот СІС для поширення недостовірного, неповного і упередженого контенту створює передумови маніпулювання суспільною свідомістю, реалізації інтересів окремих учасників інформаційної взаємодії. Незважаючи на значний рівень наукового дослідження проблем ІБД, визначення загроз ІБД в СІС і їх класифікації є актуальною. Аналіз останніх досліджень і публікацій [1-3] показав, що проведення наукових досліджень у обраному напрямку ускладнюється відсутністю нормативно-правового забезпечення, що дозволило б розробити дієві механізми впливу на інформаційний простір, ресурси, інфраструктуру та технології на державному рівні. Відомо, що взаємодія акторів віртуальних спільнот у СІС є відносно новим феноменом [1], що додатково актуалізує обраний напрямок досліджень. Метою доповіді є розроблення узагальненої класифікації загроз ІБД у СІС.

Сьогодні на завершальному етапі знаходиться підготовка Концепції інформаційної безпеки України, яка визначає загрозу ІБД як «наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері» [4]. Встановлено, що загрози національній безпеці України в СІС пов'язані із загрозами комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави. В свою чергу, такі загрози у СІС включають [4]: зовнішні негативні інформаційні впливи; інформаційний вплив на акторів; поширення суб'єктами інформаційної діяльності у СІС викривленого, недостовірного та упередженого контенту; створення, розповсюдження, передача та зберігання контенту з метою підтримки, супроводження чи активізації злочинної та терористичної діяльності.

Висновки. Встановлено, що загрози ІБД у СІС мають комунікативний характер і проявляються у сфері реалізації потреб щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації. Розробка єдиної класифікації загроз ІБД забезпечить реалізацію процесів їх аналізу, оперативного виявлення і ефективної протидії на державному рівні.

Список літератури

1. Грищук Р. В., Даник Ю. Г., Самчишин О. В. Мобільні соціальні інтернет-сервіси як один із різновидів масової комунікації на сучасному етапі // Безпека інформації. – 2015. – Т. 21. – № 1. – С. 16–20.
2. Missaoui R., Sarr I. Social Network Analysis – Community Detection and Evolution. – Switzerland : Springer International Publishing, 2014. – 272 p.
3. Пелещишин А. М. Сєров Ю. О., Березко О. Л. [та ін.] ; за ред. А. М. Пелещишина. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства : монографія. – Л. : Вид-во Львівської політехніки, 2012. – 368 с.
4. Проект Концепції інформаційної безпеки України : [електронний ресурс] / Сайт Міністерства інформаційної політики України. – Режим доступу: http://mip.gov.ua/documents/30.html (дата звернення: 03.03.2016). – Назва з екрану.

УДК 004.021

Дискретне логарифмування у скінченному полі $GF(p)$ та алгебраїчних структурах визначених над ним

Онай М. В., старший викладач кафедри програмного забезпечення комп'ютерних систем,
onay_nikolay_kpi@ukr.net
Дичка А. І. студент кафедри програмного забезпечення комп'ютерних систем,
andriydychka@gmail.com
Національний технічний університет України «Київський Політехнічний Інститут», м. Київ

Криптостійкість сучасних протоколів асиметричної криптографії ґрунтується на складності обчислення односторонніх функцій (one way function). Однією з таких функцій є дискретне логарифмування [1, 2].

На даний момент розповсюдженими є протоколи в яких математичні операції виконуються над елементами поля $GF(p)$ або над точками еліптичної кривої, що визначена над $GF(p)$, тому є актуальною задача дослідження алгоритмів дискретного логарифмування у полі $GF(p)$ та еліптичній кривій, що визначена над цим полем [2].

Елементами $GF(p)$ є всі цілі числа від 0 до $p-1$, а операції над елементами цього поля виконуються за модулем p, де p є простим числом. Еліптична крива у формі Вейєрштрасса над основним полем Галуа задається наступною рівністю:

$$y^2 = x^3 + ax + b (\mathrm{mod}\ p),$$

де p – просте число, $p \neq 2,3$ та $4a^3 + 27b^2 \neq 0$.

Задачею дискретного логарифмування у $GF(p)$ є пошук невід'ємного x, що задовольняє рівність:

$$b = a^x (\mathrm{mod}\ p)$$

при відомих $a, b \in GF(p)$. Для випадку дискретного логарифмування на еліптичній кривій елементи a та b є точками еліптичної кривої, що визначена над полем $GF(p)$.

Для розв'язання даної задачі дискретного логарифмування використовують метод Поліга-Хелмена, метод Шенкса та λ-метод Поларда. З метою проведення експериментальних досліджень було обрано систему комп'ютерної математики Sage [3], що видається з ліцензією GNU GPL. Дана система дозволяє виконувати операції над елементами скінченних полів та еліптичними кривими. Для заміру часу використовувалась функція timeit, яка за рахунок багатократного запуску дозволяє нивілювати вплив різноманітних процесів, що виконуються операційною системою та підвищити репрезентативність отриманих даних. Експериментальні дослідження проводились на віртуальній машині з операційною системою *Ubuntu 14.4* з такими технічними характеристиками CPU *VCPU 4x3.3Ghz*, оперативна пам'ять *13Gb DDR3*, що запущена на сервері з такими параметрами: CPU *Intel Xeon E3-1230 V2 4x3.3Ghz*, оперативна пам'ять *16Gb DDR3*.

Оскільки час роботи алгоритмів залежить від операндів, то для кожного поля було згенеровано 10 пар операндів (основа логарифму s операнд від якого береться логарифм) та усереднено отримані результати (таблиця 1, 2).

Таблиця 1
Час роботи алгоритмів реалізацій методів дискретного логарифмування у основному полі Галуа, мс

Довжина модуля, біт	Метод Поліга-Хелмена	Метод Шенкса	λ-метод Поларда
19	0,18	0,11	0,81
23	0,25	0,28	3,15
28	0,34	1,38	17,24
33	0,35	7,96	137,02

Таблиця 2
Час роботи алгоритмів реалізацій методів дискретного логарифмування на еліптичній кривій, що визначена над основним полем Галуа, мс

Довжина модуля, біт	Метод Поліга-Хелмена	Метод Шенкса	λ-метод Поларда
19	8,52	81,9	93,4
23	9,95	182	529
28	22,8	777	1580
33	332	9450	22000

Висновки

Отримані експериментальні результати показали, що найкращі показники швидкодії має метод Поліга-Хелмена, тому для основних полів Галуа та еліптичних кривих, що визначені над ними, рекомендовано використовувати цей метод для дискретного логарифмування. Проведене дослідження підтвердило доцільність застосування групи точок на еліптичній кривій у криптографічних протоколах, оскільки для довжини модуля до 33 біт час дискретного логарифмування на еліптичній кривій майже у 100 разів перевищує відповідний час логарифмування у скінченному полі.

Подальші дослідження слід зосередити на модифікації метода Поліга-Хелмена.

Список літератури

1. Odlyzko A. M. Discrete logarithms in finite fields and their cryptographic significance // AT&T Bell Laboratories Murray Hill, New Jersey 07974
2. Olson D. Discrete Logarithms and Elliptic Curves in Cryptography //Derek Olson and Timothy Urness Department of Mathematics and Computer Science Drake University Des Moines, IA 50311 derek.olson@drake.edu and timothy.urness@drake.edu
3. W. A. Stein Sage Mathematics Software (Version 4.7.2). The Sage Development Team, 2011 [Електронний ресурс] – Режим доступу: http://www.sagemath.org

УДК 004.7(043.2)

Засоби протидії мережному перехопленню інформації

Пількевич О.Л., студент, alexpilya@mail.ru
Науковий керівник – Павлов В.Г., доцент кафедри КСЗІ, ННІКІТ, НАУ
Національний авіаційний університет, Київ

За останніми даними кількість користувачів Інтернету нараховує 3,2 мільярда, тобто майже кожен другий використовує мережі для прийому або передачі даних. При цьому дуже актуальними стають питання захисту цієї інформації під час її переміщенні. На сьогоднішній день існують певні технології відслідковування потоків даних, які можуть бути використані зловмисниками на їхню користь або для того, щоб завдати шкоди іншим. До цих методів відноситься сніффінг мережевого трафіку з метою перехоплення деяких даних, який варто розглянути більш докладно. Сніффінг (Sniffing) або підслуховування є процес моніторингу трафіку в мережі для передачі даних та її перехоплення з метою отримання такої конфіденційної інформації, як логіни, паролі або дані про певну конфігурацію. За допомогою простого аналізатору пакетів, зловмисник може легко прочитати весь трафік, якщо він передається у вигляді відкритого тексту. На жаль, значна кількість таких популярних Інтернет-сервісів, як Telnet, POP3, HTTP, FTP передають інформацію про паролі в мережі в відкритому вигляді.

У більшості різновидів цього нападу, атакуючий є пасивним і просто спостерігає, проте в деяких варіантах зловмисник може спробувати ініціювати створення потоку даних з метою здійснення впливу на характер переданих даних.

Інструмент, який використовується для перехоплення даних, називається аналізатор пакетів. Це комп'ютерна програма або апаратний засіб, за допомогою яких стає можливим переглянути мережеві пакети цілком непомітно від того, кому вони призначені. Сніффер захоплює кожний пакет і, в разі необхідності, декодує вихідні дані пакета та аналізує його зміст відповідно до RFC або інших специфікацій.

Основним методом захисту від такого перехоплення є використання шифрування трафіку, яке може бути реалізовано на різних етапах формування інформаційних пакетів у мережі.

Віртуальні приватні мережі (VPN) надають безпечний доступ до корпоративних ресурсів шляхом створення зашифрованого тунелю через Інтернет. Широке поширення Інтернету, в поєднанні з VPN-технологій сьогодні, дозволяє організаціям економічно, ефективно і безпечно розширити охоплення своїх мереж в будь-якому місці, в будь-який час.

IPSec являє собою систему відкритих стандартів, розроблених Engineering Task Force. IPsec надає послуги захисту на рівні IP, забезпечуючи систему необхідними протоколами безпеки. Він дозволяє також перевірити цілісність пакетів, виконати автентифікацію, та забезпечити захищений обмін ключами. IPSec в основному використовується для захисту одного або декількох шляхів між двома шлюзами безпеки, між двома хостами, або між хостом і шлюзом.

Технологія WebVPN, яку запропонувала компанія CISCO, дозволяє користувачам встановити безпечний віддалений доступ за допомогою звичайного веб-браузеру. Для її застосування користувачам не потрібно програмне чи апаратне забезпечення клієнта. WebVPN забезпечує безпечний і легкий доступ до широкого спектру інтернет-ресурсів і веб-додатків з будь-якого комп'ютера, підключеного до мережі Інтернет. WebVPN використовує Secure Sockets Layer Protocol і його наступника Transport Layer Security, щоб забезпечити безпечне з'єднання віддаленими користувачам. При цьому, на відміну від IPSec, для автентифікації користувачів замість обміну ключами застосовуються сертифікати.

Висновки. Представлено загальне бачення захисту мережі від перехоплення інформації. Проаналізовані основні види загроз при передачі даних через мережу. Наведені певні міри захисту.

УДК 004.056:006.057

Концепція актуальності стандартизації в сфері безпеки інформаційних технологій

Поліщук Л.І., старший викладач, pli_80@ukr.net
Кіровоградський національний технічний університет, м. Кіровоград

Досвід світової спільноти показує, що проблема стандартизації в області безпеки інформаційних технологій є об'єктом активних дискусій. На сьогоднішній день можна з впевненістю стверджувати, що в світі відбулася переоцінка підходів до рішення цієї проблеми.

Оскільки ISO (International Organization for Standardization – Міжнародна організація зі стандартизації – існує з 1947 року) тісно працює з міжнародними організаціями і комітетами, а зокрема з Міжнародною електротехнічною комісією IEC (International Electronical Commission – існує з 1906 року), то стандарти ISO/ IEC саме і є міжнародними стандартами для різного роду електричних, електронних, електротехнічних засобів.

Україна, в тому числі, не залишається осторонь від стандартизації сучасних інформаційно-комунікаційних технологій і з 2001 року, вона також активно бере участь в роботі різних комітетів і підкомітетів ISO.

Результатом співпраці під егідою ISO стала розробка широкого спектру стандартів для інформаційної безпеки. Наведемо основні, розроблені комітетами:

1. ISO/IEC 27001:2005 Інформаційні технології. Методи забезпечення безпеки. Системи керування інформаційною безпекою. Вимоги.
2. ISO/IEC 27002:2005 Інформаційні технології. Методи забезпечення безпеки. Практичні правила керування інформаційною безпекою.
3. ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Керування ризиками інформаційної безпеки.
4. ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем керування інформаційною безпекою.
5. ISO/IEC 17799:2005 Інформаційні технології. Методи забезпечення безпеки. Практичні правила керування інформаційною безпекою.
6. ISO/IEC TR 18044:2004 Інформаційні технології. Методи забезпечення безпеки. Керування інцидентами інформаційної безпеки.

Ще одним важливим стандартом є так звані Загальні критерії (Common Criteria) — розроблений за участю урядів, визнаний у всьому світі стандарт ISO в галузі оцінювання захищеності IT-продуктів та систем. Загальні критерії передбачають сертифікацію програмних продуктів незалежною акредитованою лабораторією з обов'язковим прискіпливим тестуванням і вивченням документації.

Нажаль, наведені стандарти досі не отримали вітчизняних аналогів, що значно уповільнює процеси стандартизації національних розробок в галузі безпеки інформаційних технологій. Нині стандартизація та щонайменша уніфікація підходів до визначення якості комп'ютерних програм, засобів, систем тощо залишається досить низькою.

В Україні існують законодавчі підстави необхідної сертифікації. Але, вітчизняний сертифікат не є дійсним за межами держави. Для дійсного визнання світовою спільнотою необхідна сертифікація відповідно ISO 9001:2000 у спеціальних інституціях, таких, наприклад, як ABS Quality Evaluations (США), Lloyd's Register Quality Assurance (Великобританія), TUV (Німеччина), Bureau Veritas Quality International (Франція) та ін.

Схвалення подібних інстанцій необхідне компаніям, що пропонують товари чи послуги іноземним клієнтам, у тому числі й засобам безпеки, що прагнуть створити гідну конкуренцію зарубіжним аналогам. Ці та інші протиріччя ускладнюють процес інтеграції нашої держави у світовий інформаційний простір.

Висновки. Наше дослідження не вичерпує всіх аспектів проблеми. Подальшого вивчення потребує іноземний досвід стандартизації засобів захисту і безпеки інформаційних технологій.

УДК 004.056

Завдання інформаційної безпеки для реалізації системи електронного уряду

Понарін Д.В., студент 4-го курсу, d_ponarin@mail.ru
Науковий керівник – Халімов Г.З., д.т.н., професор
Харківський національний університет радіоелектроніки, м. Харків

Перехід державних послуг в електронний формат здійснюється як в розвинених, так і в країнах, що розвиваються, і є однією з пріоритетних цілей Організації Об'єднаних Націй. Умовою безперебійного функціонування системи електронного уряду є забезпечення необхідного і достатнього рівня інформаційної безпеки його компонентів.

Типовими джерелами загроз можна назвати наступні: свідомі дії з розкриття засобів захисту, помилки персоналу, помилки та збої інформаційних систем, вихід з ладу частин апаратних комплексів, вплив зовнішніх техногенних факторів.

Загрози, з точки зору системи документообігу, можна розділити на чотири типи:

- Загрози по відношенню до дотримання конфіденційності інформації;
- Загрози по відношенню до дотримання цілісності інформації, в тому числі дотримання цілісності документа;
- Загрози по відношенню до дотримання технології обробки (в тому числі дотримання умов юридичної значимості дій);
- Загрози відмови в обслуговуванні.

Основними технічними і технологічними методами захисту є наступні: шифрування (таємність, цілісність), хеш-функції, контрольні суми, перешкодостійке кодування, засоби ідентифікації і автентифікації (в тому числі апаратні, біометричні), реалізація моделей управління доступом: мандатна та дискреційна, сертифікація, використання аналогів власноручного підпису (перш за все ЕЦП), протоколювання дій (користувачів і автоматичних процесів).

Для забезпечення захисту інформації при її обробці в ІС, що реалізуються в рамках створюваних підсистем забезпечення інформаційної безпеки, застосовуються такі заходи:

- Захист від несанкціонованого доступу до інформації, конфіденційність і цілісність інформації;
- Захист інформації від шкідливого впливу комп'ютерних вірусів (антивірусний захист);
- Виявлення комп'ютерних атак;
- Захист інформації від витоку технічними каналами;
- Резервне копіювання і відновлення інформації.

Реалізація заходів щодо захисту інформації забезпечується комплексом засобів захисту інформації. Типовий склад комплексної системи захисту інформації повинен складається з наступних основних засобів:

- Захист інформації від несанкціонованого доступу;
- Межмережеве екранування;
- Виявлення мережевих атак;
- Аналіз захищеності;
- Криптографічний захист інформації, що передається по каналах зв'язку;
- Антивірусний захист;
- Посилена автентифікація при віддаленому доступі до ресурсів ІС;
- Захист інформації від витоку технічними каналами.

УДК 004.056.55

Дослідження проблеми генерації псевдовипадкових чисел в шифруванні

Розломій І.О., аспірантка, innulichka-best@inbox.ru
Науковий керівник – Косенюк Г.В., к.т.н., доцент
Черкаський національний університет імені Богдана Хмельницького, м. Черкаси

Стрімкий розвиток інформаційних технологій обумовлений необхідністю впровадження систем захисту інформації, які б забезпечували високий рівень інформаційної безпеки разом з підтримкою високої швидкості передачі даних каналами зв'язку. В наш час, в зв'язку з захистом конфіденційної інформації, що передається в інформаційно-комунікаційних мережах, виникла необхідність в генерації псевдовипадкових послідовностей чисел. Досить часто спеціалістам сфери інформаційних технологій в своїй діяльності доводиться працювати з випадковими числами. Найчастіше використання псевдовипадкових послідовностей зустрічається в задачах комп'ютерного моделювання, тестування та чисельного аналізу. Проте, не варто забувати і про криптографію, оскільки більшість сучасних криптоалгоритмів базуються на основі використання випадкових чисел.

Послідовності випадкових чисел (ПВЧ) грають в криптографії визначну роль, вони використовуються для формування ключових параметрів криптографічних алгоритмів, а також послідовностей шифруючих підстановок в криптосистемах. Датчики ПВЧ застосовується в криптографічних протоколах для формування ключів, при хешуванні паролів, а також в симетричних системах захисту конфіденційної інформації [1].

Криптографія і випадковість взаємопов'язані поняття, оскільки засобами криптографічних перетворень відкритий текст перетворюється в зашифровану послідовність випадкових символів. Для реалізації систем шифрування використовують ПВЧ, тому стійкість шифру в основному залежить від алгоритму формування випадкової послідовності. Завдяки можливостям сучасних компіляторів не складно генерувати ПВЧ, проте з криптографічної точки зору, вони є нестійкими [2]. Насамперед це обумовлено тим, що комп'ютери детерміновані, тобто генерують випадкові числа з певною періодичністю, яку можна передбачити. Більш надійними, ніж детерміновані генератори, вважаються ГПВЧ з джерелом ентропії, які здатні генерувати цілком непередбачувані, випадкові послідовності.

Для генерації ПВЧ використовуються генератори ПВЧ, конгруентні датчики, датчики *M*-послідовностей, нелінійні датчики ПВЧ. Також мають місце і інші, більш складні, варіанти отримання чисел для гами шифру [3]. Досить велика кількість праць присвячена вивченню і дослідженню вимог до криптостійких ГПВЧ.

Ідея використання ПВЧ знайшла своє застосування в шифрі гамування, в якому алгоритм генерації гами грає вирішальну роль. На рис.1 показано схематичне зображення алгоритму шифрування-розшифрування текстового документу методом гамування.

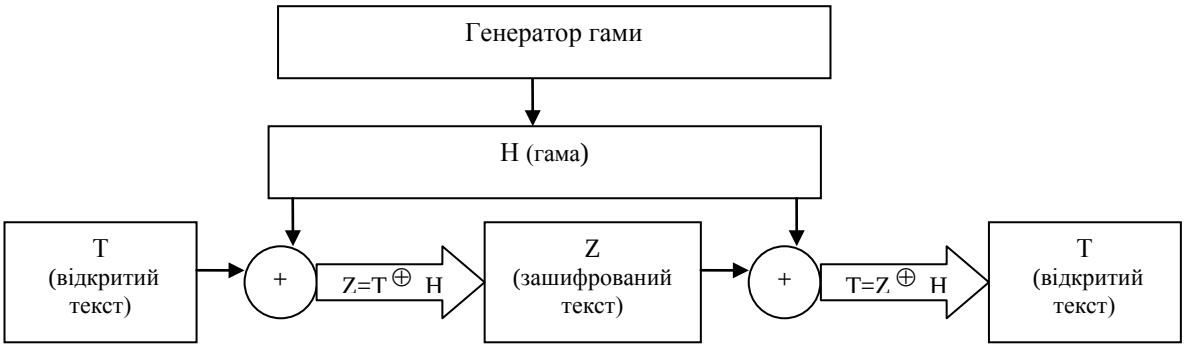


Рисунок 1 – Схема шифрування-дешифрування текстового документу методом гамування

Зазвичай, шифрувати доводиться інформацію великого об'єму, представимо її у вигляді послідовності $T=(t_1,t_2,...,t_n)$, де $t_i \in [0,1]-$ операнди-розряди, символи відкритого тексту. Згенеровану, на основі секретного ключа *k,* гаму псевдовипадкових чисел представимо у вигляді послідовності $H=(h_1,h_2,...,h_n)$, де $h_i \in [0,1]-$ символи гами. Шифрування методом гамування відкритого тексту, попередньо перетвореного в послідовність двійкових символів t_i, здійснюється шляхом додавання за модулем символів t_i з двійковими символами гами h_i.

$$Z = T \oplus H \quad (1)$$

Розшифрування тексту здійснюється аналогічним способом – накладанням символів h_i гами на зашифровану послідовність *Z.*

$$T = Z \oplus H \quad (2)$$

Стійкість шифрування методом гамування залежить від довжини гами, а також ймовірності повтору її символів. Очевидно, найстійкішим гамування буде за таких умов: всі символи гами будуть повністю випадковими, з'являтимуться в рівній ймовірності і довжина гами має бути не меншою за довжину відкритого тексту.

Зашифрований текст є достатньо складним для розшифрування, якщо гама не має бітових послідовностей, які повторюються. Гама шифру має змінюватися випадковим способом для кожного слова тексту окремо, щоб розшифрування стало складною проблемою для зловмисника [4].

За умов сучасного розвитку інформаційних технологій, забезпечення ефективності функціонування алгоритмів шифрування залишається актуальним завданням. Існуючі схеми шифрування є достатньо криптостійкими, проте мають низьку швидкість виконання криптографічних перетворень. Натомість, висока швидкість шифрування, як правило, може призвести до зниження надійності захисту даних.

Висновки. Аналіз наукової і технічної літератури показує, що можливості сучасних апаратно-технічних засобів дозволяють без особливих зусиль отримувати ПВЧ. Алгоритми шифрування, зокрема метод гамування, вимагають якісного формування ПВЧ, тобто цілком непередбачуваних послідовностей, які б відповідали певним критеріям з метою забезпечення інформаційної безпеки. Для існуючих способів генерації випадкових чисел характерна низька швидкодія, що значно впливає на швидкість шифрування. В зв'язку з цим виникає необхідність побудови нових алгоритмів шифрування без використання морально застарілих генераторів ПВЧ. Тому, доцільною, в найближчому майбутньому, буде розробка нових алгоритмів генерації ПВЧ, які б сприяли підвищенню криптостійкості шифрування.

Література

1. Казакова Н.Ф. Поэтапное тестирование и подбор составных элементов генераторов псевдослучайных последовательностей// Восточно-Европейский журнал передовых технологий. Автоматика. Вычислительная техника. Выпуск №8(44). Том 2. – 2010. – 44 – 48 с.

2. Р.М. Михерский Шифр на основе случайных чисел с неравномерным распределением// Програмні системи захисту інформації ISSN 1727-4907. Проблеми програмування. Випуск № 4. – 2011. – 90 – 95 с.

3. Калмыков И.А, Дагаева О.И. Разработка псевдослучайной функции повышенной эффективности// Известия ЮФУ. Технические науки. Выпуск № 12. Том 125. – 2011. – 160 – 169 с.

4. Авдошин С.М., Савельева А.А. Криптографические методы защиты информационных систем// Известия АИН им. А.М. Прохорова. Бизнес-информатика. Том 17. – 2006. – 91– 99 с.

УДК 004.8

Формалізація рівня загроз інформаційної безпеки підприємства

Савеленко О.К., викладач, kolodochkinaek@i.ua
Кіровоградський національний технічний університет, м. Кіровоград

Забезпечення інформаційної безпеки є важливим завданням для будь-якої організації, оскільки від збереження конфіденційності, цілісності і доступності інформаційних ресурсів багато в чому залежать якість і оперативність ухвалення управлінських рішень, ефективність їх реалізації.

Держава, регламентуючи стосунки в інформаційній сфері, не здатна виконати в повному об'ємі із завданнями забезпечення безпеки усіх суб'єктів інформаційних стосунків, однозначно відповідаючи лише за захист інформації, що становить державну таємницю. Тому в умовах різних форм власності ці завдання в повному об'ємі повинні вирішуватися керівниками організацій.

Це завдання може бути вирішене на базі експертних систем підтримки прийняття рішень, які реалізують спеціальні методики обстеження організацій і видачі рекомендацій по забезпеченню їх інформаційної безпеки [1].

При використанні апарату чітких і нечітких множин формалізований опис процесу забезпечення інформаційної безпеки організації в експертних системах підтримки прийняття рішень (СППР) можливо здійснити при послідовному визначенні наступних етапів:

- рівня загроз інформаційної безпеки;
- ресурсів організації, як об'єктів загроз;
- оцінки рівня забезпечення інформаційної безпеки організації;
- генерації рекомендацій по досягненню заданого рівня.

Розглянемо перший етап СППР, а саме, формалізацію рівня загроз інформаційної безпеки.

Загрози інформаційної безпеки в організації розділені за трьома ознаками: джерело загрози, об'єкт загрози, методи і засоби реалізації загрози. Кожна з виділених ознак містить свої характеристики, особливості, що відображають її, і загрози, що впливають на характер. Джерело загрози має дві важливі характеристики - тип і розташування; об'єкт загрози характеризується типом і метою загрози; методи і засоби реалізації загрози обумовлені особливостями джерела і об'єкту загрози.

Множина джерел загрози представлена у вигляді матриці розмірністю 3x2 :

$$I = \begin{pmatrix} I_A^{in} & I_A^{out} \\ I_T^{in} & I_T^{out} \\ I_C^{in} & I_C^{out} \end{pmatrix}, \quad (1)$$

або

$$I=\{ I_j^k \}, \quad (2)$$

де j - індекс типу джерела загрози, $j=\{A, T, З\}$, IA - множина антропогенних джерел загрози; IT - множина техногенних джерел загрози; IC - множина стихійних джерел загрози; k - індекс розташування джерела загрози, $k=\{in, out\}$, Iin - множина внутрішніх джерел загрози, $Iout$ - множина зовнішніх джерел загрози.

Множина об'єктів загроз представлена у вигляді матриці розмірністю nx3 :

$$O = \begin{pmatrix} O_1^K & O_1^Q & O_1^D \\ O_2^K & O_2^Q & O_2^D \\ O_3^K & O_3^Q & O_3^D \\ \dots & \dots & \dots \\ O_t^K & O_t^Q & O_t^D \end{pmatrix}, \quad (3)$$

або

$$O=\{O_i^m\}, \quad (4)$$

де i – індекс об’кта загрози; m – ідентифікатор цілі порушення аспекту інформаційної безпеки (ІБ); O_i^K – об’єкт з порушеною конфіденційністю; O_i^Q – об’єкт з порушеною цілісністю; O_i^D – об’єкт з порушеною доступністю; K – ідентифікатор порушеної конфіденційності; Q – ідентифікатор порушеної цілісності; D – ідентифікатор порушеної доступності.

Вважаючи, що будь-яке джерело загрози спрямоване на будь-який ресурс організації з метою порушення будь-якого аспекту ІБ, задається бінарне відношення $\rho_1 = \left(I_j^k, O_i^m\right)$ реальних пар «джерело загрози – об'єкт загрози», де $\rho_1 \in I \times O = \{(I_j^k, O_i^m) \mid I_j^k \in I, O_i^m \in O\}$.

Будь-яке джерело загрози, що спрямоване на конкретний об'єкт і має певну мету порушення аспекту ІБ, використовує для реалізації методи і пов'язані з ними засоби, що описується бінарним відношенням $\rho_2 = \left(z_e, l_q\right)$, $z_e \in Z$, $l_q \in L$, де Z – множина методів реалізації загрози; L - множина засобів реалізації загрози.

Таким чином, можна записати, що якщо на множині IxO задано бінарне відношення $\rho_1 = \left(I_j^k, O_i^m\right)$ і на множині ZxL задане бінарне відношення $\rho_2 = \left(z_e, l_q\right)$, то можливе відображення f, задаюча відповідність $\left(I_j^k, O_i^m\right) \xrightarrow{f} \left(z_e, l_q\right)$, що має наступні особливості: значення функції, які залежать від змінних I_j^k и O_i^m; умови бієкції не виконуються, оскільки не виконуються умови ін'єкції (область визначення задається парами $\left(I_j^k, O_i^m\right)$ на множині IxO, а значення функції із множини ZxL для різних елементів можуть співпадати). Відображення f є сюр’єктивним, а задавання множини пар (z_e,l_q) виконується експертними процедурами.

Таким чином, формалізований опис загроз ІБ організації матиме наступний вигляд:

$$U = \left(I_j^k, O_i^m, z_e, L_n\right), \quad (5)$$

де I_j^k - ідентифікатор джерела загрози, що характеризується типомі розташуванням; O_i^m - ідентифікатор об’єкта загрози, що характеризується типом ресурсу організації і ціллю порушення аспекту ІБ; z_e - ідентифікатор e-го методу реалізації загрози; L_n - ідентифікатор n-ї подмножини засобів реалізації загрози.

В подальшому визначається наступний етап, а саме, ресурси організації, як об'єкти загроз. Розгляд поточного і наступних етапів формалізованого опису процесу забезпечення інформаційної безпеки організації в експертних системах підтримки прийняття рішень (СППР) не розглядається, так як виходить за межі даної теми доповіді.

Список літератури

1. Королева, Н.А. Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации: моногр. / Н.А. Королева, В.М.Тютюнник. – Тамбов; М.; СПб.; Баку; Вена: Нобелистика, 2006. – 290 с.

2. Васильев В.И. Система поддержки принятия решений по обеспечению безопасности персональных данных /В. И. Васильев, Н. В. Белков. – Уфа. - Весник УГАТУ: Методы и системы защиты и нформации. – 2011. - Т. 15, № 5 (45). С. 54–65

УДК 004.057.4:004.738.5(043.2)

Забезпечення захисту інформації при її передачі в середовищі Internet

Свердлов А.І., студент, sverdlov.andrew@gmail.com
Науковий керівник – Мелешко О.О., доцент
Національний авіаційний університет, м. Київ

Використанням мережі Internet для он-лайн керування своїм банківським рахунком, покупки товарів, оплати різних послуг, вже давно нікого не здивуєш і не дивно, бо глобальна мережа є майже в кожному домі. Здебільшого користувачі не розуміють, як вона влаштована, що є безпечним, а що може становити ризики для персональних даних. Саме їх здебільшого намагаються вкрасти інтернет-злочинці. В зв'язку з цим питання захищеності інформації при передачі її по мережі Internet, привертає до себе все більше і більше уваги.

Так як інформація передається незахищеним середовищем, то найпростішим методом є її перехват. І хоча для запобіганню цьому використовується маса криптографічних протоколів, все одно не можливо стверджувати, що хоч один з них є цілком захищеним. Не виключенням став і протокол HTTPS.

Протокол HTTPS колись використовував SSLv2, протокол шифрування який вийшов ще в 1995 році і втратив актуальність вже в 1996 році. І хоча пройшло вже 20 років, виявилося, що багато серверів, досі не відключили його підтримку.

На початку 2016 року було виявлено нову вразливість, яку назвали DROWN — **D**ecrypting **R**SA using **O**bsolete and **W**eakened e**N**cryption, і яка дозволяє дешифрувати TLS - трафік клієнта, якщо на серверній стороні не відключили підтримку протоколу SSLv2 у всіх серверах, що оперують одним і тим же приватним ключем.

На момент виявлення вразливості 25% з мільйона найбільш відвідуваних веб-сайтів схильні до цієї уразливості, або 22% з усіх просканованих серверів, що використовують сертифікати, видані публічними центрами сертифікації.

Дана атака дозволяє дешифрувати TLS-трафік, маючи доступ до будь-якого сервера, що підтримує SSLv2, і використовує такий же приватний ключ, що і веб-сервер. Часто можна зустріти використання одного і того ж сертифіката для веб-сервера і поштового сервера, а також для FTPS. Схема показана на рис.1.

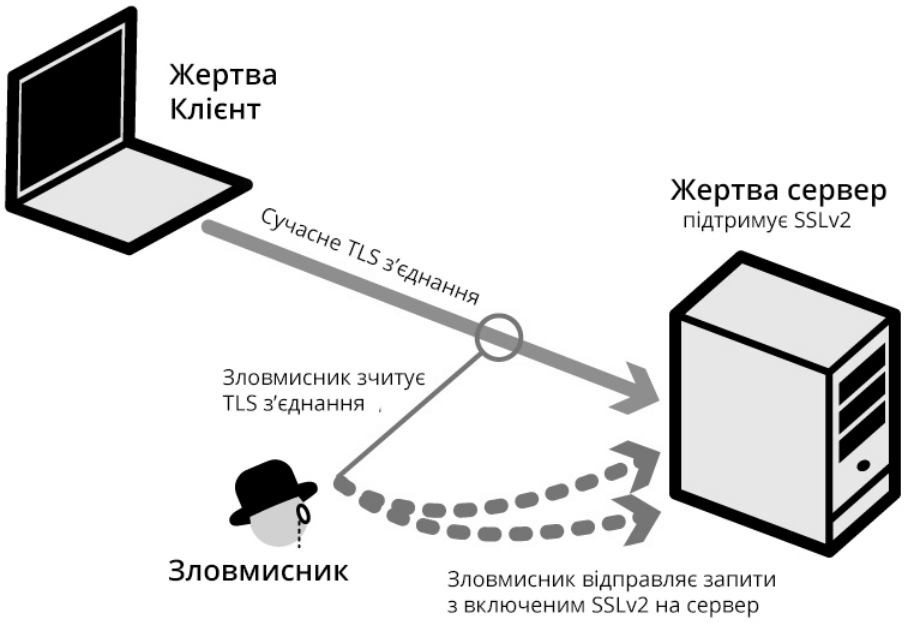


Рисунок 1 - Схема атаки DROWN

Загальний варіант атаки експлуатує уразливість в експортних шифрах SSLv2, що використовують 40-бітові ключі RSA.

Для успішного здійснення атаки в разі, якщо інформація передається без використання ефемерних ключів, узгоджених про протоколу Діффі-Хеллмана або його версії на еліптичних кривих, зловмисникові необхідно пасивно прослуховувати сотні TLS-з'єднань жертви і відправляти спеціальним чином сформовані пакети на сервер з SSLv2, що використовує такий ж приватний ключ.

Атака можлива внаслідок витоку інформації про коректність розшифровки пакета в протоколі SSLv2. Використовуючи атаку Данеля Блейхенбахера і відправляючи перехоплені клієнтські пакети з зашифрованим 48-бітовим попередніми секретом (pre-master secret), хакер зможе повністю розшифрувати одну з приблизно 900 TLS-сесій клієнта. Для виконання атаки потрібно послати близько 40000 запитів на сервер з включеним SSLv2, підбираючи ключ для слабкого симетричного шифрування на кожне відправлене повідомлення.

Крім загального випадку, існує і помітно швидший окремий випадок атаки, що експлуатує іншу помилку в OpenSSL, яка залишалася непоміченою як мінімум з початку проекту OpenSSL (1998 рік) і була випадково виявлена під час дослідження іншої проблеми 4 березня 2015 року.

Уразливість дозволяє відновлювати master secret побайтово, здійснюючи всього 1920 запитів до сервера для відновлення 128-бітного ключа.

Атака настільки обчислювально проста, що її можливо зробити на звичайному комп'ютері за хвилину.

Даній атаці піддається близько 9% серверів зі списку Alexa Top Million.

Також, атаку можна здійснити в тому числі на протокол QUIC – транспортний протокол, який використовує UDP, створений Google.

TLS-сесії, що використовують ефемерні ключі, теж уразливі, однак вимагають втручання в сесію у вигляді «людини посередині».

Щоб захиститися від цієї вразливості адміністратору серверів достатньо обновитися до найновішої версії OpenSSL з яких виключена підтримка SSLv2, в іншому випадку вимкнути підтримку вручну. Якщо немає можливості відключити підтримку SSL v2 (наприклад, на вбудованому пристрої), потрібно переконатися, що цей сервер використовує унікальний приватний ключ, відсутній будь-де ще.

Звичайно, захиститися від цієї вразливості не сильно важко, але виправляти вразливості вже після того як їх було знайдено, також не найкраща ідея. Саме тому для максимального ефекту, не можна нехтувати оновленнями до найновіших версій, заради збереження підтримки клієнтів з застарілим ПО.

Список літератури

1. DROWN Attak [Електронний ресурс]. – Режим доступу: https://drownattack.com/
2. Уязвимость DROWN в SSLv2 позволяет дешифровать TLS-трафик [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/dsec/blog/278335/
3. More than 11 million HTTPS websites imperiled by new decryption attack [Електронний ресурс]. – Режим доступу: http://arstechnica.com/security/2016/03/more-than-13-million-https-websites-imperiled-by-new-decryption-attack/
4. Дилип Н. Стандарты и протоколы Интернета / Найк Дилип; -М.: Channel Trading Ltd., 1999. – 384 с.

УДК 004.728.4:004.056

Защищенные протоколы маршрутизации в беспроводных mesh-сетях

Светайло И.О., студент 4 курса, ilsv908@gmail.com
Научный руководитель – Халимов Г.З., д.т.н., профессор
Харьковский национальный университет радиоэлектроники, г. Харьков

Mesh-сеть (WMN) – это беспроводная сеть, в которой роль маршрутизаторов и коммутаторов выполняют сами конечные узлы, объединенные по ячеистой топологии. Главным преимуществом таких сетей называют надежность и отказоустойчивость за счет отсутствия центральных узлов, выход из строя которых мог бы остановить работу сети, избыточности, способности находить новые маршруты (самоорганизация) и перестраиваться при недоступности отдельных узлов (самовосстановление). Из этого также следует скорость и простота развертывания и масштабирования, отсутствие необходимости в сложной инфраструктуре.

Одно из самых уязвимых мест mesh-сетей – протоколы маршрутизации. Это связано с широковещательной природой беспроводной связи, сложностью маршрутизации в децентрализованных динамических системах, зависимостью участников сети друг от друга при передаче данных. Используя особенности их работы, атакующий может встроиться практически в любой маршрут, нарушить работоспособность сети далеко за пределами приема/передачи подконтрольных ему узлов или полностью остановить работу отдельных участников или значительной части сети.

Исследователи предлагают ряд новых и модификации существующих протоколов с разным подходом к решению этой проблемы:

ARAN (Authenticated routing for ad hoc networks) – реактивный протокол маршрутизации, обеспечивающий обнаружение, установление и поддержание маршрута с помощью криптографических сертификатов. Он предполагает использование доверенного сервера сертификации, чей публичный ключ известен узлам. Присоединяясь к сети, узел получает сертификат со своим IP-адресом, публичным ключом, временем создания и сроком действия. При установлении маршрута узел рассылает подписанный им пакет RDP (route discovery packet) включающий, помимо прочего, его сертификат. Каждый последующий узел в маршруте проверяет подпись и сертификат предыдущего и заменяет их своими. Конечный получатель отсылает по обратному маршруту пакет REP (route reply packet) со своим сертификатом. Протокол предотвращает участие неавторизованных узлов, ложные или измененные пакеты маршрутизации, MitM-атаки. Однако, он уязвим к DoS-атакам, поскольку проверка подписи каждого пакета требует заметных вычислительных ресурсов.

SEAD (Secure efficient ad hoc distance vector) – проактивный протокол маршрутизации на основе DSDV (destination-sequenced distance vector). В нем используется цепочка значений хеш-функции для аутентификации номеров последовательностей и метрик в сообщениях обновлений таблиц маршрутизации. Протокол обеспечивает взаимную аутентификацию отправителя и получателя. Цепочки хэш-сумм гарантируют целостность метрик и номеров последовательностей. Для защиты от нарушителей, передающих те же параметры, что получили, параметры и адрес отправителя связываются с помощью дерева хэщ-сумм.

Протокол **SAR (Security-aware ad hoc routing**) использует безопасность как одну из главных метрик при выборе маршрута. Протокол предоставляет средства для усиления и измерения безопасности. SAR дополняет реактивные протоколы, такие, как AODV и DSR, включая метрику безопасности (например, наличие и уровень доверия между узлами) в сообщения маршрутизации.

SAODV (Secure ad hoc on-demand distance vector) – расширение AODV, обеспечивающее целостность, аутентификацию и неотказуемость сообщений AODV. SAODV использует цифровую подпись для защиты неменяющихся полей сообщений и хеш-цепочки – для меняющихся. Для получения и проверки публичных ключей друг друга узлам требуется механизм распределения

ключей. С увеличением мобильности узлов производительность SAODV относительно AODV заметно снижается.

ARIADNE (a secure on-demand routing protocol for ad-hoc networks) – расширение протокола DSR (dynamic source routing). В отличии от SEAD с защитой сообщений на каждом шаге, ARIADNE применяет “сквозной” подход к безопасности. Протокол предполагает наличие разделенного секрета между отправителем и получателем и использует его как ключ для аутентификации сообщений MAC-кодами. В базовом варианте ARIADNE уязвим к атаке “червоточина”.

SLRP (Secure link-state routing protocol) – защищенный проактивный протокол для беспроводных mesh-сетей и мобильных ad hoc сетей. Его задача – обеспечить безопасное обнаружение узлов и распространение информации о состоянии связей в беспроводной сети. Критическое требование SLRP – наличие асимметричной ключевой пары у каждого сетевого интерфейса каждого узла. Участники сети идентифицируются по IP-адресам соответствующих интерфейсов. Распределение ключей осуществляется группой узлов либо с применением пороговой криптографии. Работу SLRP можно разделить на три части:

- распределение публичных ключей;
- обнаружение соседних узлов;
- обновление состояния связей между узлами;

Узлы рассылают свои сертификаты в пакетах PKD (public key distribution). Последующие пакеты от отправителя проверяются таким сертификатом. Информация о состоянии связей рассылается периодически с помощью протокола NLP (neighbor lookup protocol) в виде подписанных HELLO-сообщений с MAC- и IP-адресами отправителя. NLP может генерировать предупреждения в ответ на подозрительные события (например, совпадение MAC-адресов). Для защиты от DoS-атак узлы сортируют соседей по приоритету, в зависимости от количества исходящего трафика. Главный недостаток протокола – высокая вычислительная нагрузка.

HWMP (Hybrid wireless mesh protocol) – стандартный протокол маршрутизации для сетей IEEE 802.11s, имеющий и проактивные, и реактивные свойства. Для определения маршрута он использует механизм, похожий на используемые в AODV и DSR. HWMP основан на модификации AODV, работающей на MAC-уровне – RM-AODV. Mesh-портал (узел, работающий как мост между mesh-сетью и проводной сетью) создает дерево, выступая его корнем.

BSMR (Bysantine-resilient secure multicast routing) – защищенный протокол для многоадресной рассылки. Обеспечивает безопасную рассылку сообщения от отправителя к группе получателей, если между ними существует хотя бы один маршрут без злоумышленников. Механизм аутентификации гарантирует, что только разрешенные узлы могут выполнять определенные критические действия, такие, как добавление в группу рассылки.

Список литературы

1. Jaydip Sen “Security and Privacy Issues in Wireless Mesh Networks: A Survey” [Электронный ресурс]. Режим доступа: http://arxiv.org/ftp/arxiv/papers/1302/1302.0939.pdf
2. A. Sgora, D. D. Vergados, P. Chatzimisios “A Survey on Security and Privacy Issues in Wireless Mesh Networks” [Электронный ресурс]. Режим доступа: http://aetos.it.teithe.gr/~peris/research/Wiley_Security.pdf
3. P. Papadimitratos, Z. J. Hass “Secure link state routing for mobile ad hoc networks” // Proceedings of the Symposium on Applications and the Internet Workshops, pp. 379-383, Washington DC, USA, 2003

УДК 004.056

Обзор магазинов Android приложений

Сергийчук Ю.А., Сергийчук А.В., студенты 6 курса, iurii.sergiichuk@gmail.com
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Науки 14,
каф. Безопасности информационных технологий

Согласно исследованиям компании IDC [1], Android-устройства занимают более 82% рынка на вторую четверть 2015 года, что, однозначно, превышает доли рынка мобильных устройств, работающих на базе других мобильных платформ. Однако, такая популярность платформы Android для мобильных устройств, также, как и распространенность операционной системы(ОС) Windows для настольных персональных компьютеров (ПК), означает, что Android автоматически становится основной целью [2] для злоумышленников и вредоносного программного обеспечения(ПО). Согласно исследованиям компании Pulse Secure [2], 97% всего вредоносного ПО для мобильных устройств, было написано для платформы Android.

Однако, согласно модели распространения приложения платформы Android, установка вредоносного ПО, практически всегда, невозможна без подтверждения пользователем данной установки, что означает, что практически все вредоносное ПО для платформы Android должно распространяться тем же образом, что и обыкновенные приложения – через магазины приложений.

Наиболее известным и чаще всего используемым магазином приложений платформы Android является Google Play (ранее Play Market), который поставляется в составе ОС Android, однако, этот магазин не является единственным, согласно статье Джейми Гиггса [3] на начало 2015 года существовало более 40 различных магазинов, распространяющих приложения для платформы Android.

Опираясь на количество доступных в магазине приложений и их качество, мы выделили следующие наиболее популярные магазины для платформы Android:

Google Play – более одного миллиона 970 тысяч приложений [4]

Amazon Appstore – более 400 тысяч приложений [5]

GetJar – более 800 тысяч приложений [6]

Yandex Store – более 100 тысяч приложений.

F-Droid – более 1700 open-source приложений.

Относительно же средств проверки приложений на наличие вредоносного кода для каждого из выбранных магазинов, можно обозначить следующее:

Google Play – использует автоматизированную систему проверки приложений под названием "Bounce", которую начали использовать в начале 2012 года [7]. Данная система в автоматическом режиме анализирует все добавленные в Google Play приложения и аккаунты разработчиков, пытаясь выявить признаки уже известного вредоносного ПО, а также проверяет поведение приложения в своей тестовой облачной инфраструктуре, пытаясь распознать возможные отклонения в поведении программы, которые могут быть расценены как вредоносные действия. Также Google Play в совокупности с Google Services Framework позволяет удаленное удалять уже установленные приложения [8].

Amazon Appstore – магазин компании Amazon позиционируется как магазин с более качественным контентом – каждое приложение, которое попадает в Amazon Appstore проходит ряд автоматизированных проверок и контроль качества, обеспечиваемый сотрудниками Amazon [9].

GetJar – не смотря на огромное количество приложений и пользователей данного магазина, он не предусматривает никаких проверок безопасности приложений, которые могут добавить разработчики. Согласно политике использования магазина, он не предоставляет абсолютно никаких гарантий [10].

Yandex Store – магазин компании Yandex позиционируется как хорошо защищенный магазин, который защищен модулем безопасности «Лаборатории Касперского». Каждое приложение, которое добавляется в данный магазин проходит обязательную проверку система обнаружения вредоносного ПО «Лаборатории Касперского» и сотрудниками компании Yandex [11].

F-Droid – небольшой репозиторий open-source приложений, который гарантирует, что все приложения, загруженные из данного репозитория собраны на серверах F-Droid и из исходных кодов, которые доступны на веб-сайте F-Droid. Команда разработчиков и сообщество F-Droid фильтрует добавляемые приложения и помечает потенциально-вредоносные, но не предоставляет гарантий, однако, каждый желающий может сам ознакомиться с исходными кодами всех приложений, и даже собрать их собственноручно.

Различные площадки распространения приложений Android используют различные подходы в обеспечении высокого уровня поставляемого контента и безопасности своих пользователей, такие как:

- корпоративные системы автоматизированного тестирования приложений;
- мануальную проверку каждого добавляемого приложения;
- известные и проверенные решения рынка антивирусных приложений;
- open-source модель распространения приложений, которая позволяет каждому провести анализ и аудит устанавливаемого приложения.

Однако, не смотря на все прилагаемые усилия, наиболее надежным способом защиты от вредоносного ПО для платформы Android все еще является осведомленность и внимательность пользователей мобильных устройств, так как основой архитектуры безопасности платформы Android является модель разрешений, которые пользователи и только пользователи выдают каждому установленному приложению.

[1] IDC, «Smartphone OS Market Share, 2015 Q2,» 02 12 2015. [В Интернете]. Available: http://goo.gl/2qoyex. [Дата обращения: 07 02 2016].
[2] Pulse Secure Mobile Threat Center (MTC), «2015 MOBILE THREAT REPORT,» 2015. [В Интернете]. Available: https://goo.gl/9TgDI4. [Дата обращения: 07 02 2015].
[3] J. Giggs, «The Ultimate App Store List,» 24 02 2015. [В Интернете]. Available: http://goo.gl/znByi6. [Дата обращения: 07 02 2016].
[4] AppBrain, «Number of Android applications,» 06 02 2016. [В Интернете]. Available: http://goo.gl/Jqhs0j. [Дата обращения: 07 02 2016].
[5] Statista Inc, «Number of available apps in the Amazon Appstore from March 2011 to March 2015,» 2016. [В Интернете]. Available: http://goo.gl/k75HCK. [Дата обращения: 02 07 2016].
[6] GeJjar Baltic JSC, «GetJar,» GetJar, 2015. [В Интернете]. Available: http://goo.gl/3LHro3. [Дата обращения: 07 02 2016].
[7] H. Lockheimer, «Android and Security,» Google, 02 02 2012. [В Интернете]. Available: http://goo.gl/zSk0dE. [Дата обращения: 15 02 2016].
[8] R. Cannings, «Exercising Our Remote Application Removal Feature,» 23 06 2010. [В Интернете]. Available: http://goo.gl/iYxcSV. [Дата обращения: 15 02 2016].
[9] Amazon.com, Inc, «Publishing Android Apps to the Amazon Appstore,» 15 02 2016. [В Интернете]. Available: https://goo.gl/e4C00s. [Дата обращения: 15 02 2016].
[10] GeJjar Baltic JSC, «Developers Addendum,» 09 05 2014. [В Интернете]. Available: http://goo.gl/2VpMXq. [Дата обращения: 15 02 2016].
[11] S. Malenkovich, «Защищенный магазин Android-приложений от «Яндекса»,» 25 02 2013. [В Интернете]. Available: https://goo.gl/pi2gMD. [Дата обращения: 15 02 2016].

УДК 004.49.5

Методика структурной идентификации рисков разработки программного обеспечения

Смирнов А.А., д.т.н., проф., dr.smirnovoa@gmail.com, Коваленко А.В., к.т.н., доц.
Кировоградский национальный технический университет, г. Кировоград

Используя результаты исследований, мнения экспертов, маркетинговые данные, а также базы знаний таких известных фирм как *Epam Systems* и *Nix Solutions Ltd*, идентифицируем риски разработки ПО. Основные риски разработки программного обеспечения можно представить в виде совокупности множеств организационных, управленческих, операционных, технологических, эксплуатационных, социальных и правовых рисков.

Отличительной особенностью представленной классификации является учет эксплуатационных рисков. Особенную важность эти риски приобретают в условиях повышенного уровня киберпреступности, когда пренебрежение уязвимостями программного обеспечения может привести к эксплуатационным проблемам, а зачастую и невозможности эксплуатации («краху») ПО.

Кроме этого, в условиях украинского правового поля наблюдаются отдельные случаи неадекватности и несоответствия правовым нормам действий должностных лиц государственного аппарата.

Практика ряда известных фирм-разработчиков ПО (*Nix Solutions Ltd*, и др.) показывает, что указанный фактор риска целесообразно учитывать при разработке ПО, наряду с фактором возможного изменения украинского законодательства.

Большинство из рассматриваемых рисков разработки ПО (организационные, операционные, управленческие и др.) могут оказывать непосредственное влияние как на процесс разработки ПО, так и на процесс его эксплуатации. В то же время, например, эксплуатационные риски непосредственного влияния на процесс разработки ПО не оказывают. Но пренебрежение этими рисками ведет зачастую к провалу эксплуатации ПО и потерям будущих заказов и проектов (простоям разработчиков ПО). Именно этим фактором вызвана связь между блоками «Провал при эксплуатации ПО» и «Провал при разработке ПО».

Однако, несмотря на это в целом можно выделить множество рисков непосредственно влияющих на процесс разработки ПО и множество рисков непосредственно влияющих на процесс эксплуатации ПО.

Следует заметить, что выделенные факторы в достаточной степени описывают перечень возможных рисков разработки ПО. Однако, они не дают представления о взаимном влиянии и соответственно возможном изменении конечного результата. Кроме этого приведенные множества рисков разработки ПО в разной степени влияют на конечный результат. Поэтому следующим шагом идентификации рисков разработки ПО целесообразно выполнить процедуры ранжирования и выделения наиболее приоритетных (важных) рисков разработки ПО.

Проведенные исследования показали, что для решения задачи определения взаимовлияния рисков целесообразно использовать инструмент анализа причинно-следственных связей между различными факторами и рисками, разработанный Каору Исикава (диаграмма Исикавы). В соответствии с известным принципом Парето, среди множества потенциальных причин (причинных факторов, по Исикаве), порождающих проблемы (следствие), лишь две-три являются наиболее значимыми, их поиск и должен быть организован. Для этого осуществляется:

- сбор и систематизация всех причин, прямо или косвенно влияющих на исследуемую проблему;
- группировка этих причин по смысловым и причинно-следственным блокам;
- ранжирование их внутри каждого блока;
- анализ получившейся картины.

Поэтому данный инструмент позволяет прояснить и учесть все существенные факторы, влияющие на результат разработки ПО.

Применение диаграммы Исикавы позволяет выяснить причины каких-либо проблем в организации или, например, причины возникновения эксплуатационных «багов» ПО. При этом диаграмма Исикавы имеет ряд достоинств:

- помогает наглядно показать связи между полученным результатом и вызвавшими его причинами;
- позволяет провести анализ цепочки факторов, воздействующих на проблему.

Изображение диаграммы Исикавы дает возможность получить более подробную информацию о возможности взаимовлияния различных видов риска друг на друга, что так же даст уточняющие данные для количественного анализа рисков. Однако задачу выбора наиболее приоритетных рисков диаграмма решить не может.

Для решения этой задачи в работе предлагается использовать математический аппарат многокритериальной оптимизации, основанной на локальной геометрии множества Парето.

Анализ литературы показал, что существуют, по крайней мере, три формулировки многокритериальной оптимизации, основанной на локальной геометрии множества Парето:

1. Локальная. Найти одно Парето-оптимальное решение (ближайшее к заданной начальной точке).
2. Глобальная. Найти конечное множество Парето-оптимальных решений, достаточно хорошо описывающее (покрывающее) истинный Парето-фронт.
3. Интерактивная. Найти Парето-оптимальное решение, максимально удовлетворяющее предпочтениям лица принимающего решение (ЛПР).

Проведенные исследования показали, что в процессах, построенных на принципах постоянных коммуникаций между участниками, использования «мозговых штурмов» с привлечением мнений экспертов, целесообразным представляется использование интерактивной формулировки многокритериальной оптимизации.

В этих условиях абстрактную задачу выбора наиболее важных рисков разработки ПО из имеющегося исходного множества возможных (допустимых) вариантов (решений) X можно сформулировать следующим образом.

Обозначим множество всех заранее определенных рисков разработки ПО через $S(X)$. Очевидно, $S(X)<X$. Таким образом, в задаче выбора дано множество X, содержащее, по крайней мере, два элемента, а требуется найти некоторое его непустое подмножество $S(X)$. Предполагается, что выбор производится ЛПР, в роли которого может выступать как отдельный человек, так и целый коллектив разработчиков. Для того, чтобы совершаемый выбор в наибольшей степени соответствовал достижению имеющейся цели (т.е. был «наилучшим» или «оптимальным» для данного ЛПР), необходимо в процессе выбора учитывать мнение экспертов.

Проведенные исследования показали, что в настоящее время существует множество подходов учета мнения экспертов (метод анализа иерархий, реализованный в программном продукте *EXPERT CHOICE*, метод «искусственного» отношения предпочтения, и др.) однако все они обладают существенными недостатками, главный из которых заключается в том, что, несмотря на многообразие и детальную изученность иерархий и «искусственных» отношений, крайне редко какое-либо из них можно считать удовлетворяющим конкретное ЛПР в полной мере. Характерным примером, подтверждающим данный факт является пренебрежение оценкой уязвимостей разработанного ПО (недостаточность или полное отсутствие pen-тестирования).

Таким образом, получила дальнейшее развитие методика структурной идентификации рисков разработки ПО, отличающаяся от известных построением оценки рисков разработки ПО «сверху» в виде множества, при наличии произвольного непротиворечивого конечного набора «квантов информации».

УДК 004.49.5

Алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер облачной антивирусной системы

Смирнов А.А., д.т.н., проф., dr.smirnovoa@gmail.com,
Смирнов С.А., аспирант, Дидык А.К., к.т.н., доц.
Кировоградский национальный технический университет, г. Кировоград

В данной работе отображен алгоритм, который является составляющим метода безопасной маршрутизации метаданных в облачные антивирусные системы. Помимо данного алгоритма, основными составляющими метода являются: алгоритмы формирования множества маршрутов передачи метаданных, способ контроля линий связи ТКС и модели системы нейросетевых экспертов безопасной маршрутизации.

Отличительной особенностью алгоритмов формирования множества маршрутов передачи метаданных является показатели оптимизации и вводимые ограничения безопасной маршрутизации.

Новизна способа контроля линий связи ТКС заключается в учете «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

Непосредственное использование всего найденного множества $\aleph_{баз}$ путей передачи метаданных алгоритмом формирования базового множества маршрутов передачи метаданных, не всегда возможно и оправдано. Это становится особенно очевидно в случае высокой пропускной способности хотя бы нескольких из имеющихся каналов связи, способных обеспечить выполнение требований при передаче метаданных в узлы программного сервера. Расширение такого множества приводит к увеличению таблиц маршрутизации узлов связи, усложнению процесса распределения данных и, как следствие, к снижению достоверности передачи и информационной безопасности. Поэтому возникает необходимость в нахождении такого множества маршрутов, использование которого в условиях накладываемых ограничений позволит обеспечить максимально возможную информационную безопасность, т.е. в мониторинге каналов связи и выборе из всего найденного множества $\aleph_{баз}$ путей некоторой (оптимальной) совокупности $\aleph_{вб}$ маршрутов.

Современные требования к качеству предоставляемых услуг в ТКС задаются в параметрическом виде, системой ограничений:

$$\left\{P_{иск} \le P_{иск_{доп}},\ Q_c \ge Q_{доп},\ \mathrm{T} \le \mathrm{T}_{\text{доп}}, P_{без} \ge P_{без_{доп}}\right\},$$

где $P_{иск_{доп}}$ – допустимая вероятность искажения информационных пакетов в процессе передачи; $Q_{доп}$ – допустимая вероятность приема информационного пакета за время T, не превышающее допустимое.

В то же время, в условиях повышенной киберопасности при передаче и обработке метаданных в облачных антивирусных системах, вероятность $P_{без}$ безопасной передачи данных является одним из определяющих показателей. При этом, задача безопасной маршрутизации данных трансформируется в частную оптимизационную задачу вида:

$$\left\{P_{без} \to \max,\quad при\quad P_{иск} \le P_{иск_{доп}},\ \mathrm{T} \le \mathrm{T}_{\text{доп}},\ Q_c \ge Q_{доп}\right\}.$$

Характерной особенностью алгоритма является возможность постоянного мониторинга и учета характеристик каналов связи ТКС на маршрутах в узел программного сервера.

Именно поэтому одной из основных задач безопасной маршрутизации является определение и учет характеристических параметров линий связи, определяющих возможность кибератаки и несанкционированного доступа в ТКС.

УДК 004.056.3

Створення системи забезпечення інформаційної безпеки підприємства

Тимошенко Л.М., доц., к.е.н., lmt0902@gmail.com
Одеський національний політехнічний університет, Одеса

Засоби забезпечення збереження та захисту інформації в організації, на підприємстві або фірмі відрізняються за своїми масштабами і формами. Вони залежать від виробничих, фінансових та інших можливостей підприємства, від кількості секретів, які воно охороняє, та їхнього значення. При цьому вибір таких заходів необхідно здійснювати за принципом економічної доцільності, дотримуючись у фінансових розрахунках „золотої середини", оскільки надмірне закриття інформації, так само як і халатне відношення до її збереження, можуть викликати втрату певної частки прибутку або призвести до непоправних збитків. Відсутність у керівників підприємств чіткого уявлення про умови, що сприяють витоку конфіденційної інформації, приводять до її несанкціонованого поширення.

Наявність значної кількості вразливих місць на будь-якому сучасному підприємстві, широкий спектр загроз і досить висока технічна оснащеність зловмисників вимагає обґрунтованого вибору спеціальних рішень до захисту інформації. Основою таких рішень можна вважати:

1. Застосування наукових принципів по забезпеченню інформаційної безпеки, що включають у себе: законність, економічну доцільність і прибутковість, самостійність і відповідальність, наукову організацію праці, тісний зв'язок теорії з практикою, спеціалізацію і професіоналізм, програмно-цільове планування, взаємодію і координацію, доступність у поєднанні з необхідною конфіденційністю.

2. Прийняття правових зобов'язань з боку співробітників підприємства по відношенню до збереження довірених їм відомостей (інформації).

3. Створення таких адміністративних умов, за яких виключаються можливість крадіжки, розкрадання або перекручування інформації.

4. Правомірне залучення до карного, адміністративного й іншого видів відповідальності, які гарантують повне відшкодування збитку від втрати інформації.

5. Проведення дієвого контролю і перевірки ефективності планування і реалізації правових форм, методів захисту інформації відповідно до обраної концепції безпеки.

6. Організація договірних зв'язків з державними органами регулювання в галузі захисту інформації.

Здійснюючи комплекс захисних заходів підприємства, головне – обмежити доступ у ті місця і до тієї техніки, де зосереджена конфіденційна інформація (не забуваючи, звичайно, про можливості і методи дистанційного її отримання). Зокрема, використання якісних замків, засобів сигналізації, хорошої звукоізоляції стін, дверей, стелі та підлоги, звуковий захист вентиляційних каналів, отворів і труб, що проходять через ці приміщення, демонтаж зайвої проводки, а також застосування спеціальних пристроїв (генераторів шуму тощо) серйозно ускладнять або зроблять безглуздими спроби впровадження спецтехніки.

Для надійного захисту конфіденційної інформації підприємства доцільно застосовувати наступні організаційні заходи: визначення рівнів (категорій) конфіденційності інформації, що захищається; вибір принципів (локальний, об'єктовий або змішаний), методів і засобів захисту; встановлення порядку оброблення інформації, що захищається; облік просторових факторів; облік тимчасових факторів: – обмеження часу оброблення інформації, що захищається, – доведення часу оброблення інформації з високим рівнем конфіденційності до вузького кола осіб; облік фізичних і технічних факторів.

Для створення системи захисту об'єкта і блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів необхідно здійснити низку заходів: проаналізувати специфічні особливості розташування будинків, приміщень у будинках, територію навколо них і підведені комунікації;

виділити ті приміщення, всередині яких циркулює конфіденційна інформація, і врахувати технічні засоби, використані в них.

Алгоритм створення системи забезпечення інформаційної безпеки підприємства наведено на рис. 1.

Після визначення складових інформаційної безпеки, а також визначення джерел загроз інформаційної безпеки та методів і засобів захисту конфіденційної інформації на підприємстві слід розробити алгоритм створення системи забезпечення інформаційної безпеки підприємства з наступною послідовністю дій.

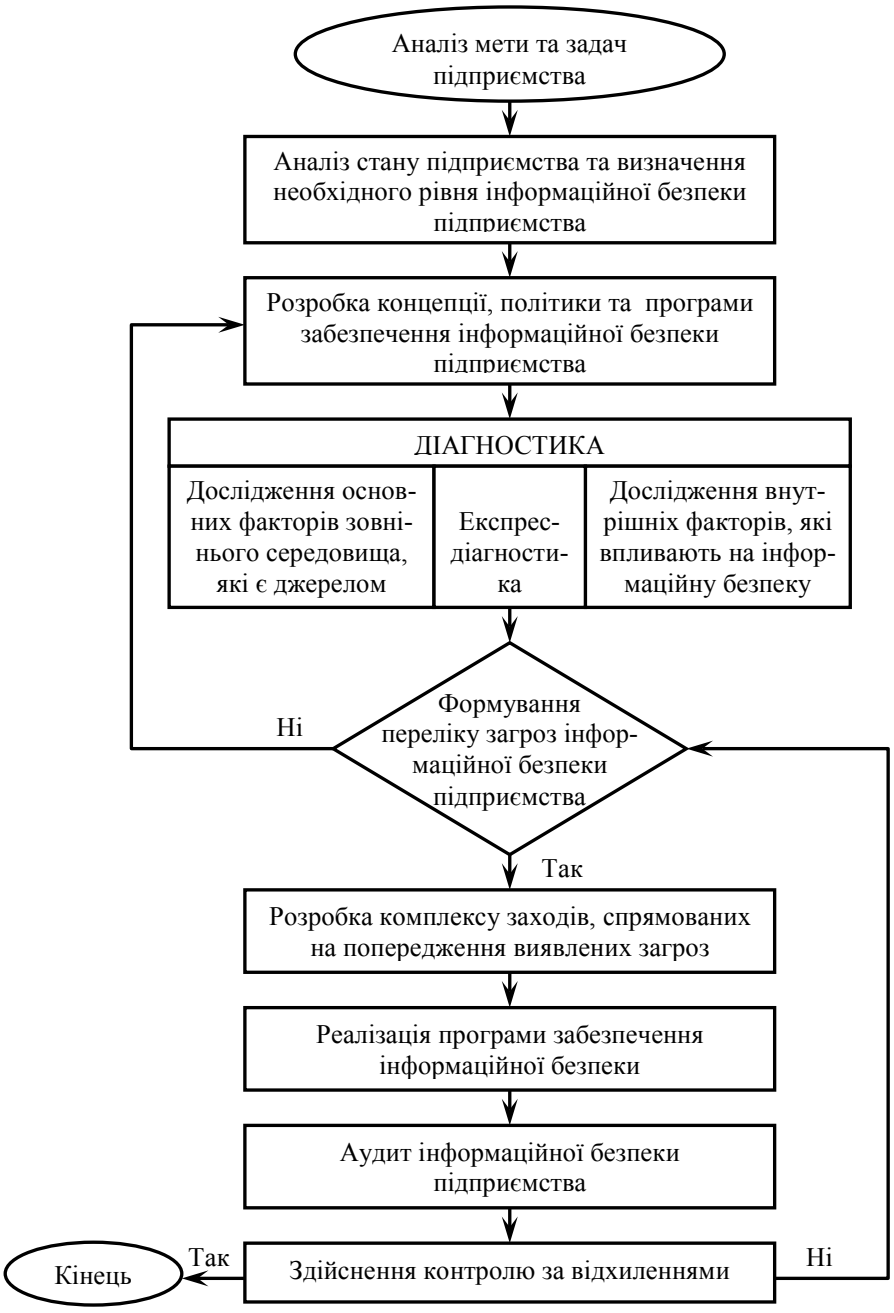


Рисунок 1 - Алгоритм створення системи забезпечення інформаційної безпеки підприємства

Запропонований алгоритм не прив'язаний до конкретних завдань та проблем, що стоять перед підприємством, тому він має універсальний характер і може використовуватися на будь-яких підприємствах різних галузей.

УДК 004.056.53(043.2)

Захист WEB-ресурсів від DDoS-атак

Хоменко І.Ю., 4-й курс, xomenko2igor@gmail.com
Науковий керівник – Павлов В.Г., к.т.н., доцент
Національний авіаційний університет, м. Київ

Швидкими темпами розвиваються технології обміну інформацією, зараз майже кожний тим чи іншим чином взаємодіє з всесвітньою мережею (англ. *World Wide Web*, скорочено: *WWW*; також: веб або тенета), а саме користується WEB-ресурсами (сайт або веб-сайт). Зараз кожна *поважаюча* себе організація, має свій веб-сайт, який може бути підвержений атаці зловмисників, що в свою чергу призведе до не бажаних збитків. Отже, потрібно захистити свій WEB-ресурс.

Одним з небезпечних видів злочинної діяльності, спрямованої на WEB-ресурси, є так звані DDoS-атаки (Distributed Denial of Service), які призводять до того, що користувачі втрачають можливість отримати доступ до ресурсів. За допомогою цих атак зловмисники можуть завдати доволі великої шкоди для власників WEB-ресурсів, та їх клієнтів.

Метою є аналіз різних підходів та методів захисту від DDoS-атак. Серед них можна виділити наступні:

- Використання ухилення і відволікання. Відведення атаки від її об'єкту шляхом використання фальшивого ресурсу (доменного імені або IP-адреси). Для відволікання можна використати ресурс-приманку, наприклад Honeypot, за допомогою якої можна вивчити стратегію зловмисника та визначити перелік засобів, які він використовує і якими можуть бути завдані удари реально наявним об'єктам.
- Застосування фільтрації і блекхолінгу. Обидва метода обмежують трафік, що виходить від атакуючих машин. Різниця між фільтрацією і блекхолінгом в тому, що при фільтрації атакуючий трафік блокується, шляхом використання списків обмеження доступу (пакетний фільтр), а при блекхолінгу перенаправляється в так звану «чорну діру» (неіснуючий сервер), тобто видаляється. Списки обмеження доступу можна отримати від компаній Arboro, CISCO, CloudShield т.д. (вони збирають переліки адрес із зараженими комп'ютерами).
- Використання зворотнього DDoS, а саме: перенаправлення трафіку, що застосовується для атаки, в зворотньому напрямку, тобто на IP-адресу атакуючого.
- Звернення до послуги компаній по блокуванню DDoS-атак. В цьому випадку трафік обмежується не на власному маршрутизаторі, а на обладнанні, наприклад, провайдера, тобто на більш високому рівні.
- Використання спеціалізованого обладнання для відбиття DDoS-атак, наприклад, DefensePro® (Radware), SecureSphere® (Imperva), Периметр (МФІ Софт), Arbor Peakflow®, Riorey, Impletec iCore та інші. Серед них можна виділити комплекс Cisco Clean Pipes в нього входять системи Cisco Traffic Anomaly Detector і Cisco Guard.

Висновки. Таким чином, запобігання DDoS-атакам – одне з головних завдань у сфері захисту інформаційних систем. DDoS-атаки, іноді, при створені системи захисту бувають недооціненими, що потім може нести за собою великі збитки. Саме тому захист від DDoS дуже актуальна тема особливо на сьогоднішній день, коли велика частина бізнес процесів (транзакцій) проходить саме через WEB-ресурси.

Список літератури

1. Методы борьбы с DDoS-атаками [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/129181/

2. Уланов А.В., Котенко І.В. Захист від DDoS-атак: механізми попередження, виявлення, відстеження джерела та протидії / / Захист інформації. INSIDE, № 1-3, 2007.

УДК 004.056.53(043.2)

Комплексний підхід до безпеки WEB-середовища

Хоменко Р.Ю., 4-й курс, xomenko2@gmail.com
Науковий керівник – Павлов В.Г., к.т.н., доцент
Національний авіаційний університет, м. Київ

Відомо, що головним призначенням комп'ютерної мережі є доступ WEB-користувача (клієнта) до інформації на WEB-ресурсі (сервері) за допомогою багаторівневої програмно-апаратної системи. В якості клієнтів найчастіше використовуються програми-браузери, що працюють на основі двох засобів – мови HTML (розробка WEB-сторінок) і протоколу HTTP, що регламентує обмін інформацією між сервером і клієнтом WEB.

Програмне забезпечення, що застосовується на WEB-серверах для підтримки WEB-сайтів, може зазнавати атаки з боку хакерів через відомі його вразливості або недостатній рівень безпеки. Далі хакер може перетворити сервер HTTP, який обслуговує сайт, у засіб для проникнення з Інтернету в локальну мережу організації до її інформаційних ресурсів.

Для здійснення подібних атак зловмисники використовують не тільки виявлені вразливості, а й цілий комплекс методів та засобів, який включає спеціалізовані програми тощо.

Відоме співтовариство OWASP (Open WEB Application Security Project) створило список з 10-и найбільш небезпечних видів атак на WEB-додатки. Цей список, який отримав назву OWASP TOP-10, містить перелік найбільш небезпечних уразливостей WEB-додатків, через які може бути нанесено великих фінансових збитків та здійснено підірв ділової репутації.

Зокрема виділяють наступні види атак: mailbombing, переповнення буфера, використання спеціалізованих програм (вірусів, сніфферів, троянських коней, поштових хробаків, rootkit-ів і т.д.), мережева розвідка, IP-спуфинг, man-in-the-middle , ін'єкція (SQL-ін'єкція, PHP-ін'єкція, міжсайтовий скриптінг або XSS-атака, XPath-ін'єкція), відмова в обслуговуванні (DoS і DDoS атаки), phishing-атаки. Для кожного типу атак є способи боротьби або ж засоби запобігання їм, які повинні використовуватися з метою підвищення рівня безпеки.

Розглянемо можливі способи захисту і боротьби на прикладі протидії міжсайтовому скриптінгу або так званої XSS-атаки, які можуть використовувати адміністраторами ресурсів:

1) Заборона включення безпосередньо параметрів GET, POST, COOKIE в генеровані HTML-сторінки.

2) Заборона завантаження довільних файлів на сервер, щоб уникнути завантаження шкідливих скриптів.

3) Збереження усіх завантажених файлів в базі даних, а не у файловій системі.

Також для захисту проти XPath-ін'єкцій та інших форм впровадження коду необхідно перевіряти всі дані, передані від WEB-сервера до служб системи зберігання даних. Слід вважати, що всі дані, які вводяться, сумнівні і перевіряти дані як на стороні клієнта, так і на стороні сервера, оскільки перевірку на стороні клієнта надзвичайно легко перехитрити. Цей підхід може бути дуже хороший для деяких WEB-додатків, які використовують REST (Representational State Transfer) або SOAP XML (Simple Object Access Protocol) – сервіси для простого доступу до об'єктів.

Висновки. Оскільки структура WEB-середовища є багаторівневою, то безпека WEB відповідно має теж розглядатися у контексті комплексного підходу. Заходи щодо захисту повинні бути реалізовані як на стороні WEB-користувача (клієнта) так і з боку WEB-ресурсу (сервера). При цьому треба враховувати такий чинник, як швидкий розвиток WEB-середовища, що потребує постійного вдосконалення засобів захисту.

УДК 004.49

Реализация защиты от основных видов атак в ОС Linux

Якименко М., магистрант 1 курса, ya_mixail@mail.ru
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Республика Казахстан

Операционная система (ОС) Linux является наиболее защищенной и более стабильной ОС, в отличие от популярной ОС Windows. Поэтому она чаще используется на серверах. А для защиты этих серверов необходимо произвести защиту от различного вида угроз. Именно такие вопросы будут рассмотрены в докладе. Рассмотрим некоторые действия по защите ОС.

1 Пользовательская политика. Главное правило заключается в том, что нельзя выполнять работы под администратором (root). Для этого создается новый пользователь, который называется «admin». Далее разрешается для admin выполнение «sudo», добавляя admin в специальную группу «sudo»

2 Настройка SSH. SSH (англ. Secure Shell – «безопасная оболочка») – это сетевой протокол прикладного уровня, который позволяет производить удалённое управление ОС, а также туннелирование TCP-соединений, например, для передачи файлов.

а) необходимо поменять порт «ssh» с 22 на любой другой, так как порт 22 чаще всего устанавливается по умолчанию. Выбираем случайное число (367), которое входит в интервал от 1 до 65535;

в) разрешаем подключение только по некоторым логинам, например, admin и для этого дописываем файл «/etc/ssh/sshd_config»;

г) запрещаем попытку входа с пустым значением пароля. Для этого в строке «PermitEmptyPasswords» и выставляем значение «no».

д) сохраняем и перезапускаем ssh-демон.

3 Реализация защиты от основных видов атак

3.1 Настройка брандмауэра. Настраиваем количество подключений с одного IP-адреса, что будет спасать сервер во время некоторых видов DOS-атак и брутфорса. Создаем правило, которое ограничивает больше 20-ти подключений к 80 порту за 15 секунд, поступающих с одного IP-адреса.

```
admin@debian:/$ sudo iptables -A INPUT -p tcp --dport 80 -i eth0 \
> -m state --state NEW -m recent --set
[sudo] password for admin:
admin@debian:/$ sudo iptables -A INPUT -p tcp --dport 80 -i eth0 \
> -m state --state NEW -m recent --update \
> --second 15 --hitcount 20 -j DROP
```

Рисунок 1 – Правило ограничения

Следующее правило ограничивает число подключений: не более 4-х подключений за одну минуту. На практике не получается авторизовать больше 1 раза за минуту для SSH, где 367 – это порт нашего ssh сервера, установленный выше.

```
admin@debian:/$ sudo iptables -A INPUT -p tcp --dport 367 -i eth0 \
> -m state --state NEW -m recent --set
admin@debian:/$ sudo iptables -A INPUT -p tcp --dport 367 -i eth0 \
> -m state --state NEW -m recent --update \
> --seconds 60 --hitcount 4 -j DROP
```

Рисунок 2 – Правило, которое ограничивает количество подключений, не более 4-х подключений за 1 минуту для SSH

3.2 Защита от сканеров портов. Защита от сканеров портов приведена на рисунке 3. Сканер портов – это такое программное средство, которое разработано для поиска хостов сети, в которых имеются нужные открытые порты.

```
admin@debian:/$ sudo iptables -A INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --
limit 1/s -j ACCEPT
[sudo] password for admin:
admin@debian:/$ sudo iptables -A INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST RST -j DROP
```

Рисунок 3 – Защита от сканеров портов

3.3 Защита от Ping of death. Защита от «Ping of death» показана на рисунке 4, после чего, сохраняем правила в брандмауэре. Ping of death – это тип сетевой атаки, во время которой компьютер-жертва принимает ложный эхо-запрос (ping) специальным образом, в результате чего, он вообще перестает отвечать на запросы (DoS).

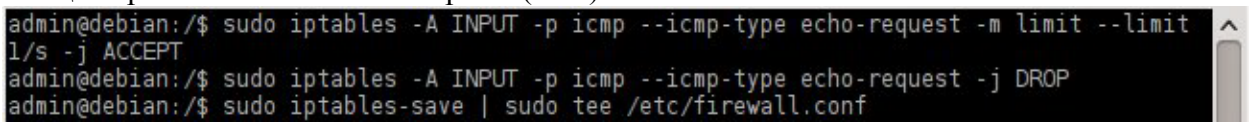


Рисунок 4 – Защита от Ping of death

3.4 Защита от SYN-флуд атак. SYN-флуд является одним из вариаций сетевых атак группы отказа от обслуживания, смысл которой заключается в посылке большого числа SYN-запросов в довольно короткий срок.

Для начала нужно проверить параметр «tcp_syncookies» – он должен быть равен «1».

Рисунок 5 – Параметр «tcp_syncookies»

Также необходимо увеличить очередь полуоткрытых соединений – «tcp_max_syn_backlog». Затем увеличиваем это значение до «20000» следующей командой:

echo "20000" > /proc/sys/net/ipv4/tcp_max_syn_backlog .

Рисунок 6 – Очередь полуоткрытых соединений «tcp_max_syn_backlog»

Вдобавок к этому, можно уменьшить время ожидания соединения «tcp_synack_retries».

Целочисленное значение, размером в 1 байт, «tcp_synack_retries» устанавливает количество попыток повтора передачи пакетов «SYNACK» для пассивных TCP соединений. Число этих попыток не должно превысить 255. Значение «5», используемое по умолчанию, соответствует приблизительно 180 секундам, отведенных на выполнение попыток организации соединения. Затем уменьшаем это значение до «1», что будет равно примерно 9 секундам (рисунок 7).

Рисунок 7 – Время ожидания соединения «tcp_synack_retries»

Целое число в файле «tcp_fin_timeout» определяет величину времени сохранения сокета после его закрытия локальной стороной в состоянии FIN-WAIT-2. Партнер может никогда не закрыть это соединение, поэтому стоит его закрыть по своей инициативе по истечении тайм-аута. По умолчанию значение этого тайм-аута составляет 60 секунд. Мы поменяем это значение на «30».

Рисунок 8 – Время сохранения сокета «tcp_fin_timeout»

Целочисленная переменная «tcp_keepalive_probes» задает число передач проб «keepalive», после которого соединение считается разорванным. По умолчанию передается 9 проб. Меняем это значение на «5».

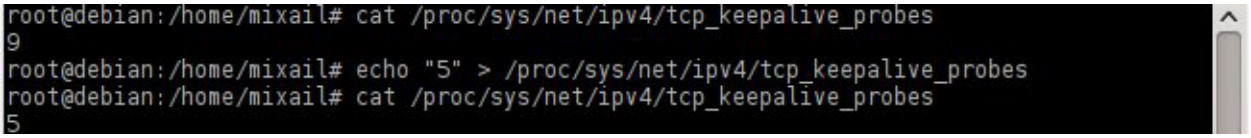


Рисунок 9 – Число передач проб «tcp_keepalive_probes»

УДК 004.056

Системи виявлення вторгнень в системи автоматичного управління підприємств на основі аналізу аномалій

Якименко М.С., доцент кафедри вищої математики та фізики, к.ф.-м.н., доцент
mykola.yakymenko@gmail.com
Кіровоградський національний технічний університет, м. Кіровоград

В останній час у захисті інформації все більшу актуальність набувають системи виявлення вторгнень (Intrusion detection system, IDS) та системи запобігання вторгнень (Intrusion prevention system, IPS). В даній роботі звертається увага на важливість наявності систем виявлення вторгнень та, зокрема, деякі види таких систем, що базуються на виявленні аномалій.

Крім загальної потреби захисту інформації в комп'ютерних системах і мережах на сьогодні в умовах інформаційної війни вторгнення в роботу підприємств несе небезпеку не тільки безпеці даних, але й роботі фізичних пристроїв. Останнім часом, зважаючи на все більшу автоматизацію, великій небезпеці підлягають енергогенеруючі, енергорозподіляючі компанії, безпеці яких приділяється багато уваги [1]. Наприклад, вторгнення в системи 3-х українських обленерго 23 грудня 2015 року призвели до відключення електроенергії не менше, ніж у 230 тис. споживачів. Ця подія привернула багато уваги у світі, так як це був перший відомий випадок успішної кібератаки на об'єкти електроенергетичної галузі.

Згідно попередніх висновків [2] розслідування, яке проводилося українськими органами сумісно із представниками ICS-CERT, та іншими міжнародними експертами, було встановлено, зокрема, що від першого втручання (за допомогою зловмисних макросів у офісних документах) до самої атаки пройшло близько півроку, протягом яких зловмисниками проводилося розвідка системи, її картографування і створення закладок. Після атаки енергопостачання було відновлено протягом кількох годин, проте автоматичні вимикачі, в яких була змінена прошивка, вийшли з ладу на значно довший час і перемикалися тривалий час в ручному режимі.

Слід відмітити, що системи захисту комп'ютерної мережі однієї із атакованих організацій, «Прикарпаттяобленерго», були (за свідченням експертів, що проводили розслідування) кращими, ніж у деяких енергорозподільчих компаніях США, що ще раз підтверджує думку, що ефективною може бути тільки побудова комплексної багаторівневої системи захисту.

В подібних ситуаціях значну користь можуть приносити системи виявлення втручань (Intrusion detection system, IDS) [3]. Не торкаючись питань розташування систем виявлення втручань (мережні чи вузлові) розглянемо їх класифікацію за методом аналізу. Виділяють 2 типи IDS: системи, що засновані на виявленні зловживань (з тих, які входять до бази даних), та на виявленні аномалій при статистичному аналізі роботи системи. Більш поширеними серед програмних продуктів є методи першої групи, але вони чутливі до регулярного оновлення баз виявлення (т.зв. вразливість нульового дня), поліморфних змін коду тощо. В реальності системи виявлення вторгнень є гібридними і поєднують як методи аналізу, засновані на виявлені зловживань, так і методи виявлення аномалій.

Перспективними виглядають системи виявлення вразливостей, що базуються на виявленні аномалій поведінки компонент системи. Інтенсивно використовуються методи [4], які використовують елементи штучного інтелекту, машинне навчання (штучні нейронні мережі, метод опорних векторів, кластерний аналіз, Байєсовські мережі, генетичні алгоритми), методи big data, а також їх поєднання. Ще однією групою є методи, засновані на нечіткій логіці [5].

Всі методи другої групи [6] є досить гнучкими до виявлення нових видів атак, проте вимагають налаштовувань під конкретну систему, часто мають велику кількість фальшивих спрацьовувань, все ще споживають багато апаратних ресурсів, вимагають часу для вивчення «нормального» стану системи.

Враховуючи хаотичну будову трафіку із властивостями самоподібності [7] запропоновано досліджувати параметри хаотичних систем, такі як, наприклад, фрактальна розмірність, параметр

Херста [8, 9], показник Ляпунова [10]. Основна ідея цих методів полягає у визначенні наскільки вказані параметри відрізняються у «нормальному» та «аномальному» станах.

Тісно пов'язаними з останніми є методи, що використовують моделювання трафіку нелінійними динамічними системами за допомогою методів теорії детермінованого хаосу [11, 12]. В роботі [12] для виявлення аномалій в роботі системи в умовах зовнішніх перешкод використовується модель брюсселятора. Для покращення роботи доцільним також є використання інших моделей динамічних систем для виявлення різних видів атак.

Для підвищення ефективності роботи систем захисту на підприємствах слід проводити більш широке запровадження тестів на проникнення, використання яких важливе також при роботі систем виявлення аномалій для перевірки адекватності різних видів моделей, може бути корисним в роботі комплексних IDS із методами машинного навчання.

Список літератури

1. Pasqualetti F. Attack detection and identification in cyber-physical systems / F. Pasqualetti, F. Dorfler, F. Bullo // Automatic Control, IEEE Transactions on. — 2013. — Vol. 58, No. 11. — P. 2715–2729
2. Alert (IR-ALERT-H-16-056-01) cyber-attack against ukrainian critical infrastructure / [Електронне джерело]. – 2016. – Режим доступу: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
3. Sharma S. Intrusion detection system: a review / S. Sharma, R. Gupta // International Journal of Security and Its Applications. — 2015. — Vol. 9, No. 5. — P. 69–76
4. Большев А. К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. дисс. на соискание научн. степени канд. техн. наук: спец. 05.13. 19–методы и системы защиты информации, информационная безопасность / А. К. Большев. – Санкт-Петербург, 2011. – 36 с
5. Корченко А. Г. Построение систем защиты информации на нечетких множествах / А.Г. Корченко. — К.: МК-Пресс, 2006
6. Agrawal S. Survey on anomaly detection using data mining techniques / S. Agrawal, J. Agrawal // Procedia Computer Science. — 2015. — Vol. 60. — P. 708–713
7. Fiore U. Network anomaly detection with the restricted Boltzmann machine / U. Fiore, F. Palmieri, A. Castiglione, A. De Santis // Neurocomputing. — 2013. — Vol. 122. — P. 13–23
8. Sheluhin O. Detection of anomalies in network traffic using the methods of fractal analysis in real time / O. Sheluhin, A. Pankrushin // T-Comm-Телекоммуникации и Транспорт. — 2014. — Vol. 8, No. 8. – P.108-112
9. Басараб М. А. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов // Вопросы кибербезопасности. — 2014. — No. 4 (7). – С. 30-40
10. Ren X. Fractal Lyapunov exponent based anomaly detection of network traffic. / X. Ren, H. Wan, others // International Journal of Advancements in Computing Technology. — 2012. — Vol. 4, No. 11. – P. 275-282
11. Palmieri F. Network anomaly detection through nonlinear analysis / F. Palmieri, U. Fiore // Computers & Security. — 2010. — Vol. 29, No. 7. — P. 737–755
12. Семенов С.Г. Аппроксимация технологии функционирования компьютерной системы в условиях внешних воздействий моделью брюсселятора с возмущениями в виде динамического хаоса / С.Г. Семенов, А.Ю. Можаев, С.Ю. Гавриленко // Системи обробки інформації. — 2014. — No. 4. — С. 188–191

Секція 2.
Програмування та інформаційно-коммунікаційні технології

УДК 654.16:004.057

Метод побудови сучасної стільникової мережі на базі технології SDN

Абакумова А.О., студент, a.a.a@ua.fm
Науковий керівник – Одарченко Р.С., к.т.н., доцент
Національний авіаційний університет, м. Київ

У сучасному світі, бізнес у сфері інформаційних технологій пред'являє все більші вимоги до гнучкості і масштабованості комп'ютерних мереж. При цьому мережа в класичному її вигляді (управління через командний рядок і конфігураційні файли) стає обмежуючим фактором розвитку обчислювальної інфраструктури. Класичні підходи до вирішення проблем, наприклад, на основі віртуалізації мереж, не відповідає рівню розвитку віртуалізації серверів і систем зберігання даних. Традиційні мережі насамперед статичні і не відповідають швидкій динаміці розвитку сучасного IT бізнесу. Можливості масштабування традиційних мереж не відповідають вимогам великого бізнесу і сервіс провайдерів, а розподілене управління пристроями традиційних мереж занадто складне і не ефективне. Як результат спостерігається картина, що традиційні архітектури мереж стають неефективні в динамічних середовищах.

Необхідна нова технологія або підхід до побудови інформаційних мереж яка дозволяє вирішити згадані вище проблеми. Така технологія є і зветься Software Defined Networking або скорочено SDN.

Перетворення за допомогою нових технологій. SDN вже зарекомендувала себе як розумний вибір для використання в дата-центрах, корпоративних мережах та мережах Інтернет-провайдерів – тобто там, де об’єми трафіку є значними. В сучасних GSM-мережах українських стільникових операторів об’єми трафіку є порівняно невеликими. Але після переходу до мереж третього та четвертого покоління, вони зростуть в сотні разів. Крім того, мережа значно ускладниться внаслідок необхідності утримання обладнання для одночасного функціонування GSM, UMTS і LTE. Тому краще вже зараз знайти рішення для більш простого і ефективного управління мережею, яке і пропонує SDN.

Технологія SDN передбачає поділ функцій управління мережею і функцій передачі даних. Така архітектура дозволяє виділити з мережевого обладнання рівень управління і зробити його програмованим (програмно-визначеним або програмно-конфігурованим). При цьому базова інфраструктура передачі даних також відділяється від мережевих сервісів і додатків. Такий підхід дозволяє винести управління мережею на окремі централізовані обчислювальні ресурси (SDN-контролери), які обслуговують всю інфраструктуру в цілому. В результаті для додатків, що використовують мережеві функції, вся інфраструктура може бути представлена у вигляді єдиного "логічного" комутатора/маршрутизатора. Координацію діяльності розробників в області відкритої архітектури SDN, а також розробку стандартів і специфікацій для пов'язаних з нею технологій виконує міжнародна організація Open Networking Foundation (ONF).

Метод побудови транспортної SDN-мережі з застосуванням OTS. Програмно-конфігуровані мережі можуть докорінно змінити оптичні транспортні мережі. SDN дозволить застосовувати централізований контроль над мережею, забезпечить її програмованість та автоматизацію надання різних сервісів для різних QoS. Тому ONF проводить розробку OTS (Open Transport Switches), які працюють як посередники між контролером та оптичним комутатором. OTS взаємодіє з контролером через протокол OpenFlow, а для взаємодії з оптичним комутатором використовується специфічний командний синтаксис для конкретного комутатора.

В оптичній мережі OTS, що під’єднаний до комутатора, отримує відомості про параметри цього комутатора і передає їх до контролера. Контролер отримує інформацію про кількість каналів, пропускну здатність, параметри QoS тощо. Таким чином контролер отримує повне бачення ресурсів мережі.

Внутрішні модулі OTS передають параметри апаратного забезпечення контролеру, повідомляють контролер про зміни стану каналу, здійснюють моніторинг продуктивності. OTS представляє собою сервер з встановленим на нього віртуальним програмним комутатором. Його внутрішня структура зображена на рис. 1.

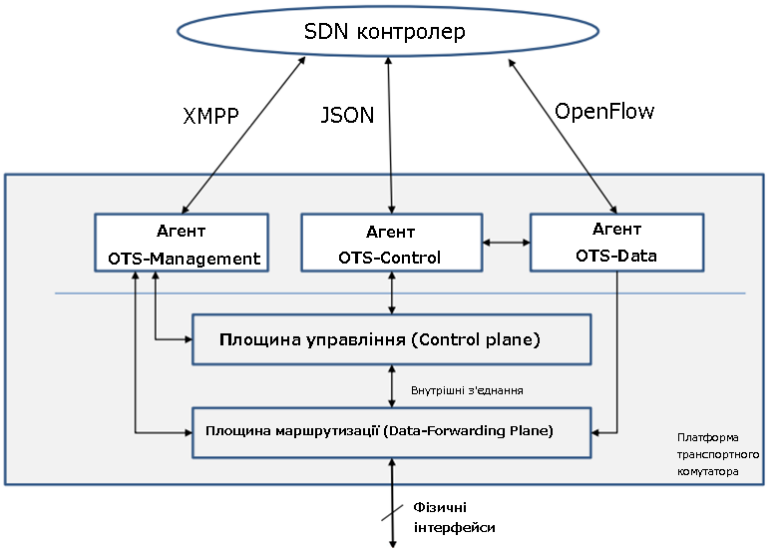


Рисунок 1 – Логіка побудови Open Transport Switch

Система управління з використанням OTS може працювати в двох режимах: явному (explicit) і неявному (implicit).

При використанні явного режиму роботи кожен транспортний комутатор має призначений для себе OTS. Тому мережевий контролер контролює напряму кожен транспортний комутатор в мережі. Такий режим роботи є більш ефективним, адже всі можливості протоколу OpenFlow та програмних додатків (а отже і переваги SDN) можуть використовуються в повному обсязі. Але при цьому реалізація такого режиму є набагато дорожчою і в деяких випадках може бути надлишковою.

При неявному режимі роботи OTS з'єднуються лише з тими комутаторами, що знаходяться на краях доменів. При цьому також використовуються існуючі сигнальні протоколи та протоколи маршрутизації всередині транспортних доменів. Контролер керує лише тими комутаторами, що під'єднані до OTS напряму. Всередині доменів маршрутизація здійснюється протоколами транспортної мережі.

Переваги побудови програмно-визначених мереж на базі технології SDN:

- повна програмованість мережі за рахунок відділення рівня управління трафіком від рівня передачі даних і перенесення функцій управління на виділені обчислювальні ресурси;
- максимально ефективне використання пропускної спроможності мережевого обладнання шляхом оптимізації пересилання мережевих потоків;
- масштабованість, яка забезпечує збільшення числа логічних мереж без зниження продуктивності вже існуючих віртуальних конфігурацій;
- підвищення безпеки за рахунок "наскрізного" управління захисними політиками в кожному мережевому пристрої для окремих потоків;
- збільшення надійності функціонування мережі за допомогою централізованого управління конфігурацією мережевих параметрів на рівні сесій, користувачів, пристроїв і додатків.

Висновки. В наше сьогодення постала проблема неефективності традиційних архітектур стільникових мереж в динамічних середовищах. Таким чином запропонована стільникова мережа, побудована на базі технології SDN, котра дозволяє створювати сучасні стільникові мережі, на яких легко можна переходити від стандарту до стандарту (GSM-UMTS-LTE-…) і надавати новітні послуги в найкоротші терміни.

UDC 004.652

Approaches towards effective websites designing

Basyuk T.M., Ph.D., associate professor, basyuk.ism@gmail.com
Lviv Polytechnic National University

Introduction. Statement of the problem. The position of web site as a search result is a very important factor that directly affects both its effectiveness and therefore the ability to attract more visitors. Thus, well-conducted search optimization contributes to its display in the top search engine ranking. Achievement of these goals is only possible if a thorough knowledge of algorithms and ranking skillful application of technology optimizing search engines, which is impossible without a detailed review of the problems of the industry, analysis of the basic methods and basic estimation algorithms.

The peculiarity of the analysis and promotion of web sites is that they allow to analyze the basic characteristics of the websites and to draw the attention of developers and owners to potential problems of optimization in order to increase positions in the search. However, the known means [1,2] do not provide mechanisms of comprehensive analysis of websites that directly affect their efficiency. Given that the prerequisite is to use a set of methods and tools to analyze and form the basis for "conglomerate" that will allow practically implement tasks in the field of decision support in the analysis and promotion of websites.

Analysis of literature. As a result of the research and analysis publications [1,3], the availability of certain components and stages of work appears to be special features of today's search engines that must be considered in the design of systems analysis and promotion of websites, namely the collection and processing of data (includes tools for resource analysis via search engines); indexation of the results (drawing for each page resource inverted index file); search information (analysis query entered by the user); rankings resources (the location of the "most useful" Internet resources in the top positions of search issue). Given these factors, the important objectives of the study are: the definition of the main approaches of analysis and web site promotion and development of recommendations on its implementation with the usage of modern programming technologies.

The main results of research. When designing the application the critical task which is necessary to be solved is to determine all functions of the developed product, communication interface between modules and components for solutions to ensure system uptime. The system architecture provides a combination of developed components that make up the module and sets the context within which following design projects are taken. Architecture development requires the adoption of such design decisions: the creation of the program modules and database management.

Creating a program module determines the allocation of a set of individual components is interconnected and has a well-defined interface connections with other components of the program. They define the shape of the interactions between them, but do not have connections to their internal structure. Given that the projected program must consist of original block modules.

Managing databases will be implemented in two aspects: managing internal and external databases. Internal databases in the storage system are considered to be the internal structure of the program in the main memory. However, files will allow them to appeal from the side of many users and easily transfer them to different platforms. In turn, external database (stored in external memory) will be used to store user data, since these data types are not easily structuring and have low information density.

As a result of conducted study the following main stages of designing effective websites were identified: semantic core designing, preparation of texts website (copywriting), code optimization, references, monitoring and analysis of results.

Semantic core designing lies in the selection of search phrases, with the help of which the popularization of Internet resources and their distribution on the site will be performed. In general, it is a complete set of words and phrases that describe a particular object and its properties. The right semantic core designing is important for search engine optimization, because it is based on search engine construction, without which the promotion is not possible. While carrying out this procedure there are

three groups of queries: high, medium and low frequency. Belonging of request to a particular group is determined by the corresponding number of made by users within a month.

Preparation of texts website (copywriting) – lies in preparation of texts, attractive for visitors and also optimized for search engines. There are several types of copywriting: simple and complex, often called rewriting.

Under the site code optimization is understood as the technical process concerning the reduction of code size, which is transmitted to users and search engines at startup. Optimizing the code has significant advantages, including: reducing the size of pages and accelerate their load; reducing the load on the server hosting that positively affects its stability (especially important for projects with a high level of attendance). The placement of links belongs to the "external factors" of optimization and without consideration of their promotion can not be successful in competitive subjects. Moreover, this work should be conducted regularly and consist in the creation of external "a reference environment" and display the required text around references, i.e. the text that matches a catalog.

Monitoring and analysis of the results lies in the constant control of the Internet resource position in search results for all queries and analysis of selected changes occurring. This procedure allows responding quickly to changes in the ranking algorithms of search engines, evaluate and promptly make the necessary adjustments.

The main processes that will take place in these approaches are the following:

– *parameters website analysis* - is the complex analysis of parameters of the web site, its Google PR and Yandex TCI indicators, stock directories (DMOZ) and the number of indexed pages;

– *choice of recommendations for promotion* - lies in gathering of analyzed information and recommendations on choosing a website optimization;

– *display of the results* - is a combination of the results and display of information about a website with recommendations for promotion.

Detailed analysis of process parameters online resource is shown in Fig. 1.

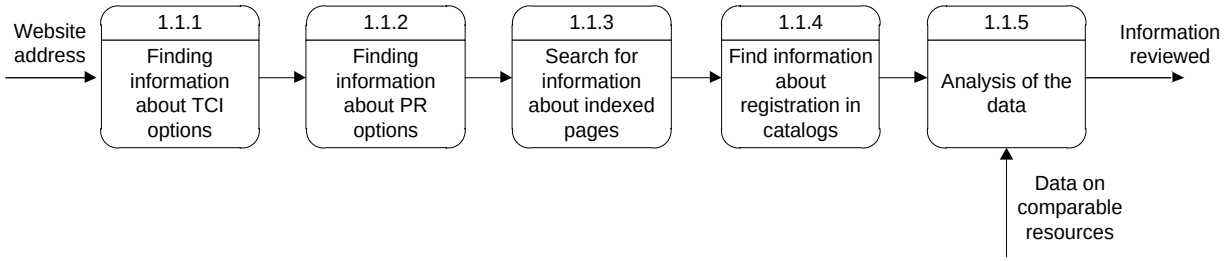


Fig. 1. Details of the process "Analysis of the resource"

Detailing of the process demonstrates the process of searching for information on the parameters of the website and is an integral part of the analysis and promotion of websites.

Conclusion. In the article the approaches to system design popularizing websites are proposed. The approach will allow to: apply new adaptive algorithms for determination of resource relevance; use interactive elements in created system; simplify administration of websites; increase competitiveness and informational content of resource.

References

1. Grappone J. Search Engine Optimization (SEO): An Hour a Day / J. Grappone – United States: Wiley Publishing Inc., 2013. – 435p.

2. Basyuk T.M. Stages of search engine optimization website /T.M.Basyuk// Proceedings of the XII International Conference MEASUREMENT AND CONTROL IN COMPLEX SYSTEMS (MCCS - 2014). (ISBN 978-966-2462-66-1) – Vinnytsia: 14-16 October 2014. – P. 89.

3. Enge E. The Art of SEO (Theory in Practice) / Eric Enge, Stephan Spencer, Jessie Stricchiola – United States: O'REILLY., 2012. – 694p.

УДК 004.93'12

Метод запобігання повторного знаходження обличчя у системах виявлення облич

Дикуха Б.О., студент 6-го курсу, borisdykuha@rambler.ru
Національний технічний університет України «Київський Політехнічний інститут», м. Київ

Сучасні програмні та апаратні рішення з розпізнавання зображень, визначення та відслідковування об'єктів знаходять все більше застосування у різних системах безпеки, візуального контролю за об'єктами, системах наведення і т. і. Так, наприклад, розпізнавання використовується в системах безпеки, в пошукових системах поліції, чи в більш близьких для простих людей соціальних мережах. Щодо методів виявлення облич, найбільш оптимальним в співвідношенні якість/швидкодія [1] вважається метод Віоли-Джонса [2, 3]. Але цей метод має ряд недоліків, в числі яких те, що він не може виявляти обличчя, що нахилені більш ніж на 10-20 градусів. Цю проблему намагався вирішити Масаюкі Танака, розробивши систему виявлення з поворотом зображення і перевіркою наявності очей, носа і рота на обличчі [4]. Але його система має недолік – можливе подвійне спрацьовування системи на одне й те саме обличчя, яке виявляється на зображенні під різними кутами. Крім того, зустрічались випадки подвійного виявлення облич навіть в частковому методі Танаки, який лише перевіряв наявність очей, рота і носа без повороту зображення. Для усунення цього недоліку пропонується метод, який базується на маскуванні облич при їх виявленні. Метод Танаки при кожному положенні зображення після його повороту виявляв обличчя, потім на *всіх* виявлених обличчях виявляв очі, рот і ніс, після чого відсіював обличчя, на яких було менш ніж 2 елементи з 4 і повторював ці дії під іншими кутами, використовуючи *те ж саме зображення* на кожному кроці. Ідея запропонованого методу полягає в тому, що після виявлення облич на зображенні відбувається *послідовна* перевірка кожного обличчя на наявність 3 елементів з маскуванням області обличчя чорним кольором при їх наявності і подальша робота вже з *замаскованим зображенням*. Таким чином, якщо помилково кілька разів було виявлене одне обличчя, то елементи цього обличчя зможуть виявитись лише один раз, а отже тільки одне таке виявлення залишиться після відсіву. Це дозволяє запобігти повторному виявленню одного й того ж самого обличчя.

Функціональна модель процесу обробки зображення з використанням запропонованого методу має наступний вигляд.

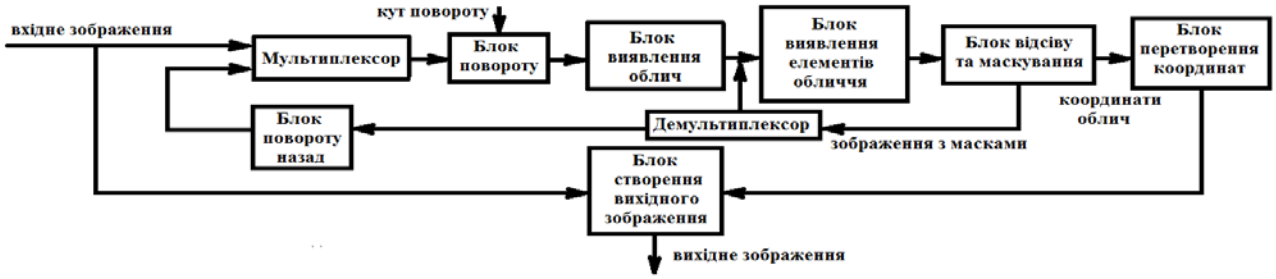


Рисунок 1 - Функціональна модель процесу обробки зображення та виявлення облич

Для обробки зображення та вирішення задачі виявлення облич оператору необхідно подати на вхід моделі зображення, на якому виявлятимуться обличчя та величину кута повороту, з яким зображення буде обертатися під час виявлення. Так як стандартний метод Віоли-Джонса виявляє обличчя під нахилом до 10-20 градусів, оптимальний кут повороту – 15 градусів (так як системі виявлення достатньо буде визначати обличчя з нахилом 7,5 градусів вліво і вправо).

Алгоритм роботи згідно функціональної моделі виглядає наступним чином.

1. На вхід подається зображення і проходить на блок повороту через мультиплексор, який потрібен для переключення джерела вхідних даних – вхідне зображення/ блок повороту назад.

2. Блок повороту повертає зображення проти годинникової стрілки на значення, кратне вхідному значенню куту повороту.

3. Повернуте зображення приходить на блок виявлення облич, в якому за допомогою методу Віоли-Джонса виявляються вірогідні обличчя в анфас.

4. Координати вірогідних облич приходять у блок виявлення елементів обличчя, в якому в областях з вірогідними обличчями шукаються очі, рот і ніс.

5. Блок відсіву та маскування оцінює наявність очей рота та носа на одному з вірогідних облич. У випадку наявності менш ніж 3 з 4 елементів, робиться висновок про відсутність обличчя по даним координатам, і координати видаляються. В іншому випадку робиться висновок про наявність обличчя, координати зберігаються, а на їх місці ставиться маска – прямокутник чорного кольору, який завадить подальшим пошукам використовувати очі, ніс та рот вже виявленого обличчя.

6. В разі наявності інших вірогідних облич, зображення з маскою через демультиплексор знов іде на блок виявлення елементів обличчя.

7. По завершенню відсіву і маскування всіх вірогідних облич, зображення з масками через демультиплексор іде на блок повороту назад, що повертає його до початкового положення, тобто за годинниковою стрілкою, після чого від зображення відрізаються зайві частини, що виникають при поворотах.

8. В такому вигляді зображення через мультиплексор йде на використовуваний у пункті 2 блок повороту і повертається на наступний кут, що кратний вхідному значенню кута повороту.

9. Знов виконуються вищеописані дії по виявленню облич, їх елементів, відсіву не-облич, маскуванню облич доти, доки всі можливі кути не будуть опрацьовані.

10. В цьому випадку, координати всіх знайдених на зображені облич ідуть на блок перетворення координат, який потрібен тому, що координати отримуються під різним кутом. Тому, по-перше, координати приводяться до одного базису, по-друге, повертаються навколо нього за годинниковою стрілкою на кут, на який було повернуте зображення при виявленні координат.

11. Перетворені координати облич і чисте вхідне зображення подаються на блок створення вихідного зображення, в якому навколо виявлених облич малюються прямокутники.

Для перевірки працездатності запропонованого методу було створено обчислювальну модель у Matlab та проведено ряд обчислювальних експериментів, які показали, що у випадках подвійного виявлення облич при використанні методу Масаюкі Танаки, запропонований метод виявляв обличчя тільки один раз.

Отже запропонований у роботі метод вирішує задачу запобігання повторного виявлення одного і того ж обличчя за допомогою маскування виявлених облич. Метод є удосконаленням методу Танаки, що доповнив метод Віоли-Джонса можливістю визначати обличчя під будь-якими кутами. Але метод Віоли-Джонса має і інші недоліки, що потребують усунення для покращення якості виявлення. До таких недоліків можна віднести, наприклад, неможливість коректного виявлення облич на зашумлених, затемнених чи засвічених зображеннях.

Список літератури

1. Татаренков Д. А. Анализ методов обнаружения лиц на изображении // Молодой ученый. – 2015., №4.– С. 270-276

2. P. Viola, M. J. Jones. Rapid Object Detection using a Boosted Cascade of Simple Features // proceedings IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 2001). - 2001, vol. 1. - pp.511–518

3. P. Viola, M. J. Jones. Robust real-time face detection // International Journal of Computer Vision. – 2004, vol. 57, no. 2. - pp.137–154

4. M. Tanaka. Face parts detection [Електронний ресурс]. – Режим доступу: http://www.slideshare.net/masayukitanaka1975/face-partsdetection

УДК 004.05:658.51

Визначення властивостей команди ІТ-проекта для обґрунтування вибору методології управління розробленням програмних продуктів

Доренський О.П., викладач, bmkntu@ukr.net
Кіровоградський національний технічний університет, м. Кіровоград

ІТ-галузь України стрімко розвивається. При цьому її левовою частиною є програмне забезпечення (ПЗ), реалізація якого здійснюється колективами фахівців – командами ІТ-проектів – з невід'ємним процесом управління розробленням ПЗ, який володіє невизначеністю. Для її зниження і забезпечення ефективності виконання ІТ-проекта використовуються методології [1], кожна з них є специфічною та неоднорідною [2]. Тому вибір методології управління конкретним ІТ-проектом є ключовою функцією менеджера, для виконання якої слід крім оцінок [2] здійснювати оцінювання ресурсу колектива виконавців. Адже він постійно набуває або втрачає певні ознаки, характеристики, властивості, що викликає невизначеність та ускладнює процес управління розробленням ПЗ.

Таким чином, постає задача визначення властивостей команди ІТ-проекту з метою обґрунтування вибору методології управління розробленням програмних продуктів.

Досягнення сформульованої мети роботи можливе за допомогою представлення команди ІТ-проекта, як соціальної організації [3], у вигляді системи та її формалізації на основі теоретико-множинного підходу [4]: $S = \{M_S, L_S, K_S\}$, де M_S є підкласом множин елементів системи S, L_S – підклас множин, які утворюються в результаті розподілу S на піделементи; K_S – підклас таких множин, в які система S сама входить як елемент. Оскільки команда ІТ-проекта є складною системою, яка розвивається, відповідно до праці [5] отримана теоретико-множинна модель володіє наступними властивостями та характерними особливостями: унікальність і непередбачуваність поведінки системи в конкретних умовах; здатність адаптовуватись до змін умови середовища, зовнішніх і внутрішніх завад; принципова нерівноважність; здатність протидіяти ентропійним тенденціям та проявляти негентропійні тенденції; нестаціонарність окремих параметрів та стохастичність поведінки; здатність і прагнення до цілісності; здатність виробляти варіанти поведінки та змінювати власну структуру, виходити на новий рівень еквіфінальності, зберігаючи цілісність і основні властивості; неоднозначність використання понять.

В роботі визначено властивості команди ІТ-проекту для обґрунтування вибору методології управління розробленням програмних продуктів шляхом експертного оцінювання [2]. Перспективою подальших досліджень є розвиток інформаційної моделі вибору методології управління ІТ-проектами [2], як моделі синтезу експертної оцінки, шляхом її доповнення інформаційною моделлю 2-го виду. Практична цінність результатів полягає у доцільності їх використання для забезпечення ефективності менеджменту ІТ-проектами.

Список літератури

1. Селиховкин И. Управление ИТ-проектом / Иван Селиховкин. – Спб.: PM, 2010. – с. 190.

2. Доренський О. П. Інформаційна модель вибору методології управління життєвим циклом програмного забезпечення інфотелекомунікаційних систем [Текст] / О. П. Доренський // Сучасні інформаційно-телекомунікаційні технології: Міжнар. наук.-техн. конф., 17-20 лис, 2015 р. : матеріали наук.-техн. конф. – Т ІІІ. – Розвиток інформаційних технологій. – К.: Державний університет телекомунікацій, 2015. – С. 114-116.

3. Тарнавська Т. В. Генеза поняття «система» [Текст] / Т. В. Тарнавська // Духовність особистості: методологія, теорія і практика. – 2011. – 6 (47). – С. 129-139.

4. Коваленко І. І. Вступ до системного аналізу: Навч. посіб. [Текст] / Коваленко І. І., Бідюк П. І., Гожий О. П. – Миколаїв: МДГУ ім. Петра Могили, 2004. – 148 с.

5. Денисов А. А. Современные проблемы системного анализа: Учебн. [Текст] / А. А. Денисов. – СПб.: Изд-во Политехнического университета, 2009. – 304 с.

УДК 004.75

Использование сетевых хранилищ в мобильных приложениях

Вдовенко Е.А., бакалавр, l.vdovenko@mail.ru
Научный руководитель – Ступак Г.В., ст. преп. каф. АТ
Донецкий национальный технический университет, г. Красноармейск

Облачные технологии широко используются в современном мире и полезны как для обычных пользователей, так и для разработчиков программного обеспечения. Наиболее известны сервисы, которые используются как сторонние хранилища, что удобно при небольшом объеме памяти на устройстве или если необходимо получить удаленный доступ к файлам. Рейтинг данных хранилищ по популярности в Украине [1] представлен в таблице 1.

Таблица 1 – Рейтинг использования сетевых хранилищ

Рейтинг	Хранилище	Рейтинг	Хранилище	Рейтинг	Хранилище
1	Google Disk	4	iCloud	7	SpiderOak
2	Dropbox	5	Copy	8	Mega
3	Облако Mail.ru/Яндекс.Диск	6	Box	9	OneDrive

Для разработчиков созданы специальные облачные платформы, которые предоставляют возможность разработки и выполнения приложений и хранения данных на серверах, расположенных в распределенных дата-центрах. Наиболее популярны в Украине Microsoft Azure, De Novo, Amazon [2]. Использование облачных сервисов разработчиками проиллюстрировано на рисунке 1.

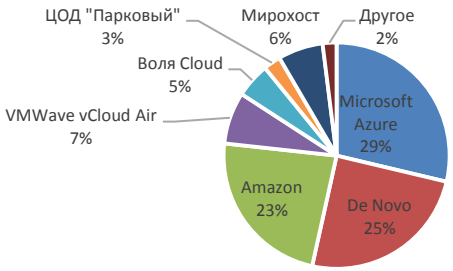


Рисунок 1 – Распространение облачных сервисов в среде разработчиков

Одной из причин, по которой данные технологии набирают всё большую популярность, является вытеснение персональных компьютеров смартфонами. По данным компании Киевстар, за 2015 год количество смартфонов в сети увеличилось на 34% или на 2,38 млн и к концу году составило 9,367 млн. пользователей [3]. При этом, согласно проведенному опросу [4], в ходе которого в течении недели нами было опрошено 445 респондентов со всей Украины, наблюдается следующая картина (рисунок 2)

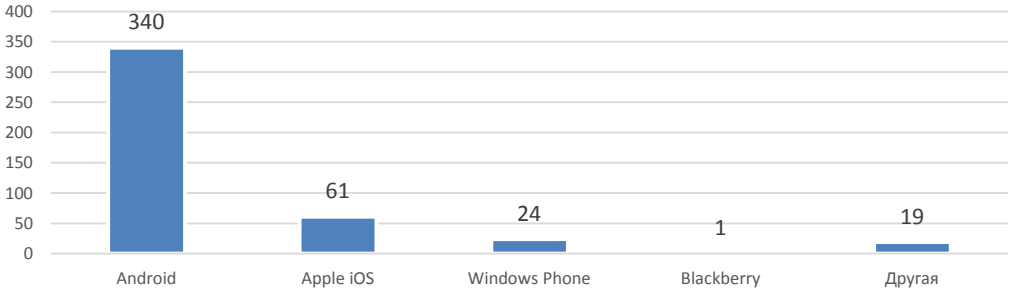


Рисунок 2 – Распределение операционных систем среди мобильных устройств

Исходя из приведенной выше диаграммы, следует, что платформы с OpenSourse доминируют, благодаря чему разработчики имеют полную свободу действий, включая использование облачных технологий при создании мобильных приложений, таких как:

– приложения для доступа к пользовательскому аккаунту сервиса облачного хранилища. Наиболее распространенным пример, создан для удобства получения доступа пользователю к своим данным, хранящимся в «облаке»;

– медиаплееры, с помощью которых пользователь может прослушивать музыку или смотреть видео, расположенные в любом из своих облачных хранилищ;

– музыкальный сервис в «облаке». Предоставляет пользователю возможность составить свой плейлист и прослушивать его без траты памяти на устройстве;

– видеонаблюдение. В данном приложении видео, записанное с камер пользователя, сохраняется сразу в «облако», и пользователь может наблюдать за происходящим с любой точки мира в режиме реального времени;

– приложения для бизнес-клиентов. Созданы для удобства пользователей, которые сотрудничают друг с другом и находятся на расстоянии: без лишних затрат времени и пользуясь удобным интерфейсом они могут делиться необходимыми отчетами, данными, графиками и др.

– онлайн-игры. Разработчики стали внедрять облачные технологии при создании онлайн-игр для мобильных устройств, чтобы оптимизировать работу приложения и уменьшить потребляемые ресурсы мобильного устройства.

Процентное соотношение использования облачных хранилищ и технологий в смартфонах, по данным нашего опроса [4] выглядит следующим образом:

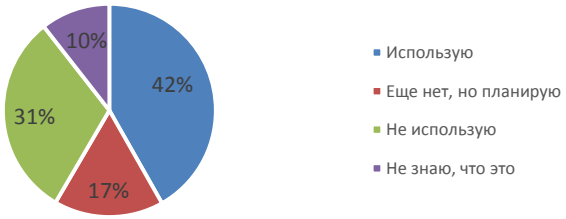


Рисунок 3 – Тенденции использования облачных технологий пользователями

Существует еще множество примеров использования облачных технологий в мобильных приложения, поэтому можно с уверенностью сказать, что данные технологии упростят пользование смартфоном пользователю. «Облако» обеспечивает не только экономию памяти устройства, удаленный доступ к файлам, но и надежность данных, так как при потере или поломке мобильного устройства файлы, хранящиеся в облаке останутся не тронутыми, зайдя с нового устройства на свой аккаунт пользователь снова сможет получить доступ к своим файлам.

Исходя из доводов, приведенных в статье, и проведенного социологического опроса, можно сделать вывод о том, что с каждым годом все большую актуальность будут приобретать сетевые сервисы распределенного хранения и обработки информации. Дальнейшие исследования будут направлены на изучение и оптимизацию ресурсов облачных хранилищ.

Список используемых источников

1. Топ-10 облачных хранилищ 2016 года [Электронный ресурс]. – Режим доступа: http://fornote.net/2016/01/top-10-oblachny-h-hranilishh-2016-goda/
2. Украинские облака выросли на 47% [Электронный ресурс]. – Режим доступа: http://igate.com.ua/news/7111-ukrainskie-oblaka-vyrosli-na-47
3. За 2015 рік кількість смартфонів у мережі Київстар збільшилася на 2,38 млн [Электронный ресурс]. – Режим доступа: http://www.kyivstar.ua/kr-620/press_center_new/news/?id=56224
4. Соцопрос: Насколько Вы используете возможности Вашего смартфона? [Электронный ресурс]. – Режим доступа: https://goo.gl/SF9nVa

УДК 681.518

Контроль качества работы беспроводной сети передачи данных в системах удаленного управления динамическими процессами

Волков А.Е., м.н.с., alexvolk@ukr.net, Волошенюк Д.А., м.н.с., Комар Н.Н., м.н.с.
Научный руководитель – д.т.н., проф. Павлов В.В.
Международный научно-учебный центр информационных технологий и систем НАН Украины и МОН Украины, г. Киев

Широкое распространение беспроводных информационно-телекоммуникационных технологий уже стало реальностью сегодняшнего дня.

В последние годы во всем мире происходит бурный рост числа беспроводных сетей передачи данных, используемых как в масштабе отдельных предприятий (локальные сети), так и в качестве связующей компоненты корпоративных и государственных сетей. Мощный стимул такого роста – появление новых стандартов, регламентирующих работу беспроводных сетей.

Как известно, в беспроводных сетях в качестве среды распространения сигнала используются радиоволны и работа устройств и передача данных в сети происходит без использования кабельных соединений. В связи с этим на качество работы беспроводных сетей влияет большее количество различного рода помех.

Проблема повышения производительности компьютерной сети весьма актуальна. На практике реальная скорость приема/передачи данных оказывается существенно ниже, чем битовая скорость, поддерживаемая используемой сетевой технологией. Особенно остро эта проблема стоит в беспроводных сетях. Реальная пропускная способность беспроводной компьютерной сети зависит от используемой технологии, количества абонентов в сети, протяженности и качества каналов связи, уровня электромагнитных помех, погоды, используемого сетевого оборудования, протоколов и многих других факторов.

Например, при воздействии электромагнитных помех происходит искажение передаваемой информации. Этот факт обнаруживается с помощью анализа контрольной суммы сетевого пакета. Если пакет был искажен, то он отбрасывается принимающей стороной. В результате получатель не отсылает передатчику подтверждение об успешном приеме, а, следовательно, отправитель выполнит повторную передачу этого пакета. Таким образом, чем больше длина сетевого пакета и чем выше вероятность возникновения битовой ошибки, тем меньше производительность компьютерной сети.

Основным фактором, влияющим на качество работы компьютерных сетей, является сетевая задержка при передаче пакетов данных. Результаты предыдущих исследований показали, что использование существующих научно-технических решений в компьютерных сетях распределенного управления скоростными циклами прикладных процессов не обеспечивает качественного контроля и управления передачей данных при наличии задержек передачи пакетов данных по сети.

Нами предлагается идея применения сетецентрических и нейронных сетевых технологий для контроля качества работы беспроводной сети. Основная научно-техническая идея построения систем контроля и распределенного управления широким классом прикладных процессов, а именно передачей данных, в глобальных просторах информационных сетей на основе сетецентрической технологий заключается в формировании команд распределенного управления путем моделирования в ускоренном масштабе времени динамики прикладного процесса совместно с моделированием процесса формирования команд управления по данным о текущем состоянии прикладного процесса. Это позволяет компенсировать задержки, ошибки и искажения передачи пакетов по сетям.

Для проведения необходимых исследований работы сетевых технологий и линий связи, применения сетецентрических и нейросетевых технологий, был создан, и предлагается способ контроля маршрута и определения качества передачи информационных данных через Wi-Fi-сеть.

Был разработан компьютерный алгоритм и программа, которые определяют маршрут передачи данных, параметры работы сети, задержки и потери пакетов данных. А также, локализуют точку маршрута передачи с наибольшими задержками и потерями, и предлагают альтернативный, более качественный, маршрут передачи данных.

Пример полученных практических результатов по качеству работы сети показан на рисунках 1 и 2. На графиках показана зависимость скорости передачи и приема данных при разном количестве пользователей от времени.

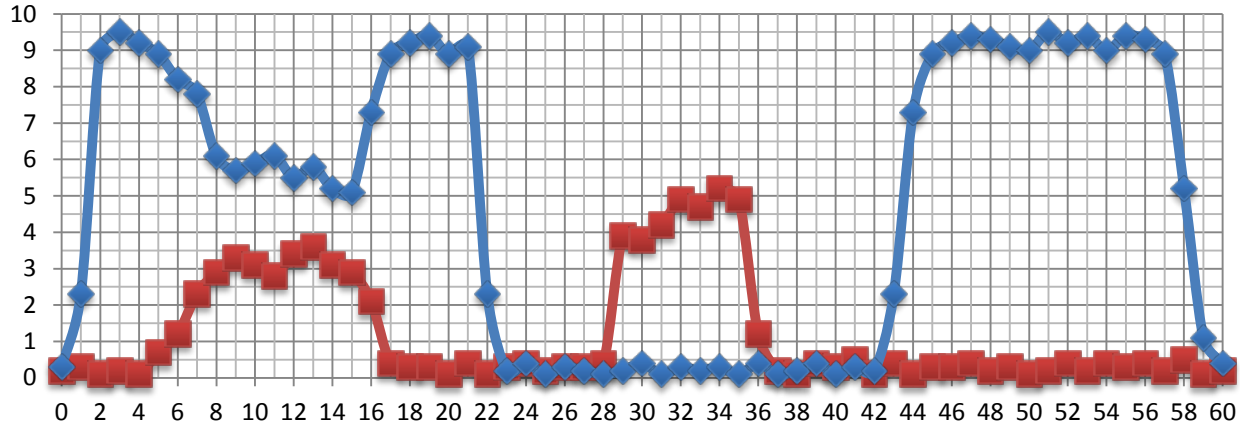


Рисунок 1.

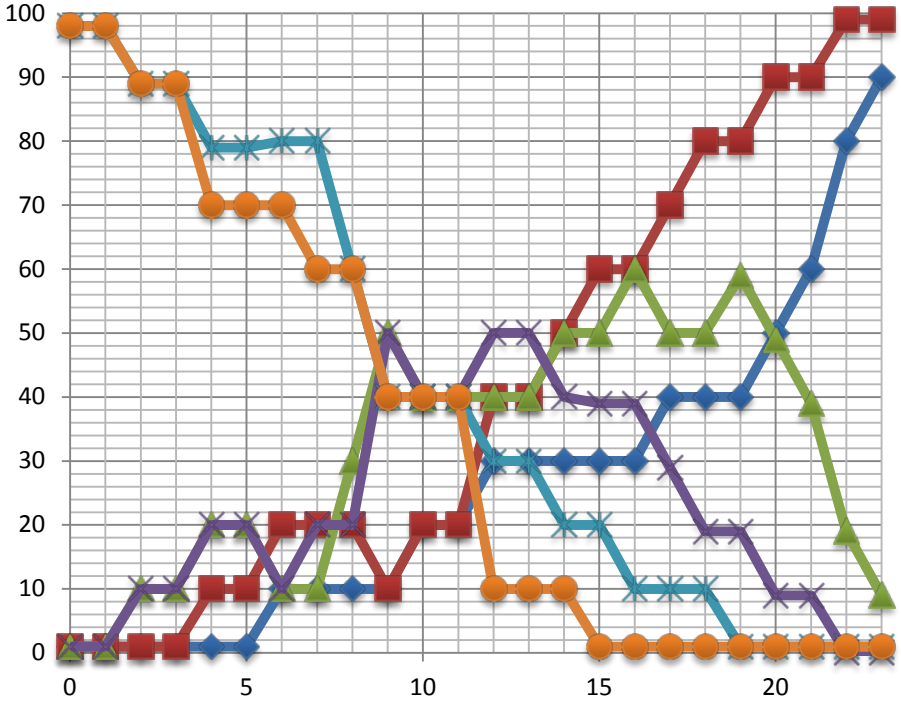


Рисунок 2.

В выводах можно отметить, что учитывая и беря за основу проблему качества работы авиационной сети и необходимость ее улучшения переходом на новые принципы и технологии передачи данных, был разработан способ контроля маршрута и определения качества передачи информационных данных через проводную Интернет-связь, который позволяет: определить маршрут передачи данных через Интернет, параметры работы сети, задержки и потери пакетов данных; локализовать точку маршрута передачи с наибольшими задержками и потерями; предоставить альтернативный, более качественный, маршрут передачи данных. Данный способ был положен в основу разрабатываемой сетецентрической системы управления и контроля передачи информационных данных в моделях удаленного управления воздушными кораблями.

УДК 621.396.67

Сравнительный анализ допустимых и реальных потерь беспроводных сетей стандарта LTE в пригороде

Дейнеко Д.В., студент, danildey@mail.ru
Научный руководитель – Шарапова Е.В., к.т.н.
Харьковский национальный университет радиоэлектроники, г. Харьков

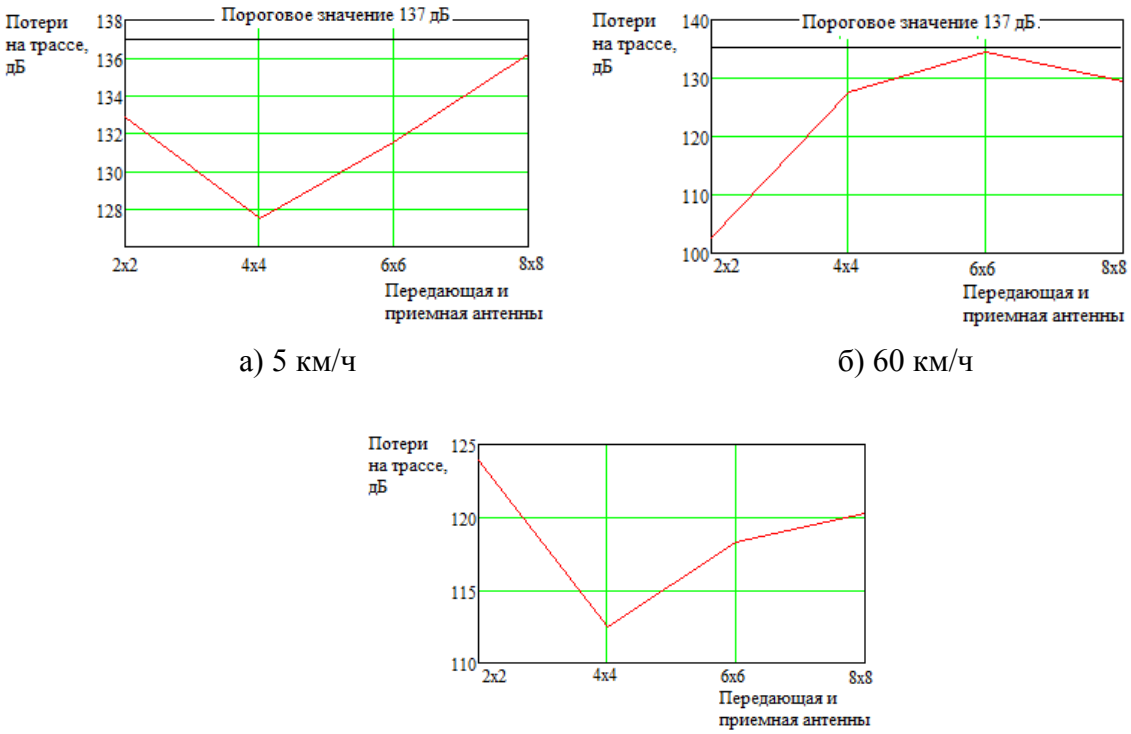
В последние годы значительно увеличивается количество пользователей и объемы передаваемой информации. Поэтому важную роль в каналах связи сейчас играет пропускная способность (ПС) и помехозащищенность. Одной из технологий, позволяющей решить вопрос повышения ПС и помехозащищенности является стандарт долгосрочной перспективы Long Term Evolution (LTE) и его улучшенная версия LTE-Advanced партнерского проекта 3GPP (3rd Generation Partnership Project) [1]. В основе данных стандартов лежит связка технологий пространственной обработки Multiple Input Multiple Output (MIMO) и ортогонального частотного мультиплексирования Orthogonal Frequency Division Multiplexing (OFDM). Крайне важным вопросом в настоящий момент является обеспечение качественной связи не только в городе, но и в сельской местности и пригороде. В больших городах активно занимаются расширением инфраструктуры, оборудования и обеспечением хорошего покрытия. При этом в сельской местности качество каналов связи ожидает желать лучшего.

Цель работы состояла в проведении моделирования и статистической оценке учета потерь в каналах связи стандарта LTE и LTE-Advanced построенных на базе MIMO систем в условиях пригорода.

Обобщая математические модели для описания каналов можно выделить детерминированные, структурно-детерминированные и стохастические модели. Существует ряд стохастических моделей для цифровых систем передачи информации – это двухлучевая модель, экспоненциальная модель, модель Salesh-Valenzuela, модель Джейкса и лучевая модель радиоканала (ЛМРК).

Новизна предложенного подхода по сравнению с известными работами (например [2]) заключается в том, что модель ЛМРК применена для статистической оценки потерь на трассе распространения каналов связи стандарта LTE и LTE-Advanced.

Для моделирования использовался стандарт 3GPP TR 25.996, где для работы выбрана ЛМРК. Для проведения расчетов, построения зависимостей и получения численных результатов выбраны следующие исходные данные каналов связи стандарта LTE и LTE-Advanced: расстояние между БС и абонентским терминалом 315 м; рабочая частота $2x10^9$ Гц; высота подвеса антенны БС 32 м; высота подвеса антенны абонентского терминала 1.5 м. Моделирование проводилось с учетом распространения радиоволн в условиях пригорода для различной скорости движения абонентского терминала. Основываясь на теорию анализа MIMO каналов связи стандарта LTE и LTE-Advanced, с помощью ЛМРК были получены зависимости потерь на трассе распространения от конфигурации антенных элементов на передающей и приемной стороне систем связи. Полученные зависимости были получены для трех скоростей движения абонентского терминала: скорость движения человека 5 км/ч (рис. 1а), скорость движения транспортного средства в городе 60 км/ч (рис. 1б) и скорости движения транспортного средства на трассе 150 км/ч (рис. 1в).



а) 5 км/ч

б) 60 км/ч

в) 150 км/ч

Рисунок 1 – Потери на трассе при разной скорости абонентского терминала

Полученные данные по результатам моделирования потерь при различной конфигурации антенной системы на передающей и приемной стороне MIMO канала и учетом скорости движения абонентского терминала показывают, что в условиях пригорода наименьшие потери достигаются при количестве антенных элементов 2x2 и скорости движения абонента 60 км/ч. Полученные данные по значениям потерь для сельской местности хорошо коррелируют с результатами, приведенными в [2]. Анализируя их совместно с данными проведенного моделирования, можно прийти к выводу, что при скорости абонента в 5 км/ч и количестве антенных элементов на передатчике и приемнике 6x6 потери достигают пикового значения по отношению к максимально допустимому в 137 дБ.

Выводы. На основе ЛМРК был смоделирован канал связи LTE на базе MIMO систем имитирующий условия распространения в пригороде и получены значения потерь на трассе. Новизна предложенной методики по сравнению с известными работами заключается в подходе, который оценивает потери в каналах связи стандарта LTE и LTE-Advanced не исключая скорость движения абонентского терминала. Результаты проведенных исследований и математическое моделирование представляет интерес для разработчиков систем передачи информации и разработчиков абонентских устройств.

Список литературы

1. 3GPP TS 33.401 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture; (Release 8).

2. Дюсенова О. С. Исследование использования новых стандартов сотовой связи и широкополосного доступа LTE и WIGIG для предоставления услуг Triple Play [Текст] / О. С. Дюсенова, О. Н. Пищин, Г. С. Павленко // Молодой ученый. — 2013. — №5. — С. 45-49.

УДК 681.324

Умови застосування визначення фрактальної розмірності трафіку мережі

Дрєєв О.М., к.т.н., викладач каф. ПЗІ, *drey_sanya@ukr.net*
Кіровоградський національний технічний університет, м. Кіровоград

В роботі розглянуто процес визначення фрактальної розмірності числової послідовності утвореної за результатами моніторингу трафіку мережі. Фрактальна розмірність використовується в ряді задач прогнозування змін трафіку, а також для прийняття рішень в системах захисту інформації. Тому задача точного визначення фрактальної розмірності є актуальною.

Переважна більшість джерел [1-4], при дослідженні можливостей щодо прогнозування трафіку мережі, використовує різноманітні методи визначення фрактальної розмірності числової послідовності рівномірних вимірювань в часі параметру трафіку. При цьому більшість засобів отримання фрактальної розмірності використовує середнє квадратичне відхилення.

Розглянуто випадкову величину x з розподілом щільності ймовірності $f(x)$, та математичним сподівання 0. Для імітування використання пошуку середнього квадратичного відхилення, розглянуто послідовність $y_i = x_{2i} + x_{2i+1}$. Функція розподілу щільності ймовірності для y матиме вигляд: $p(y) = \int_{-\infty}^{\infty} f(x) f(x-y) dx$. Для такої щільності доводиться що середні квадратичні відхилення мають відношення D(y)=2D(x), що відповідає критерію Хірста H=0,5 та фрактальної розмірності F=1,5. Тому, для довгих послідовностей визначення критерію Хірста дають близькі значення до 1,5 незалежно від виду розподілу випадкової величини.

Для перевірки теоретичних результатів побудовано програмне забезпечення. Проведено числові експерименти, для послідовностей різної довжини (до 20000) з різними розподілами. Експериментально встановлено, що використання послідовностей більше за 3000, дають оцінку показника Хірста 0,5. Результат збігається з зауваженнями в [5].

Висновки. При виконанні дослідження доведено незалежність фрактальної розмірності числової послідовності, при оцінюванні якої використовується квадратичне відхилення, від функції розподілу і завжди складає 1,5. Теоретичні результати підтверджено числовими експериментами для рівномірного, нормального розподілів випадкової величини та для розподілу Парето, при використанні послідовностей з кількістю елементів більших за 5000.

Список літератури

1. Нейман, В.И. Самоподобные процессы и их применение в теории телетрафика / В.И. Нейман // Тр. МАС. – 1999. – № 1 (9). – С. 1–15.

2. Можаев А.А. Фрактальный анализ процессов, структур и сигналов: коллект. монография / [Р.Э. Пащенко, А.М. Сотников, А.А. Можаев и др.]; под ред. Р.Э. Пащенко. – Х.: ЭкоПерспектива, 2006. – 348 с.

3. Можаєв О.О. Метод прогнозування фрактального трафіка / О.О. Можаєв, Г.А. Кучук, О.В. Воробйов // Радіоелектронні і комп'ютерні системи. – No6(18). – 2006. – С. 181-188.

4. Кучук Г.А. Фрактальный гауссовский шум в трафиковых трассах // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 3. – С. 91 – 99

5. Федер Е. Фрактали: Пер. с англ.-М.: Мир, 1991. - 254 с.

УДК 517.9:539.3

Комп'ютерне моделювання пружно-пластичного циліндричного тіла з урахуванням пружних параметрів, які залежать від температури

Дьомічев К.Е., старший викладач, demichevk@mail.ru
«Європейський університет», м.Черкаси

Температурне поле для ізотропного тіла у випадку врахування тепла, що виділяється в процесі його деформування під дією температурного та силового навантаження, визначається шляхом розв'язання нестаціонарного рівняння теплопровідності при певних початкових і граничних умовах

$$\frac{\partial T}{\partial t}=\frac{1}{H_1H_2H_3}\left\{\frac{\partial}{\partial\alpha^1}\left(a\frac{H_2H_3}{H_1}\cdot\frac{\partial T}{\partial\alpha^1}\right)+\frac{\partial}{\partial\alpha^2}\left(a\frac{H_1H_3}{H_2}\cdot\frac{\partial T}{\partial\alpha^2}\right)+\frac{\partial}{\partial\alpha^3}\left(a\frac{H_2H_1}{H_3}\frac{\partial T}{\partial\alpha^3}\right)\right\}+W_*\ , \qquad (1)$$

де $W_\bullet$ - функція розсіювання або питома потужність внутрішніх джерел теплоти, $a=\dfrac{\lambda(T)}{c_v\rho}$ - ізохорна температуропровідність, яка для термочутливих матеріалів залежить від температури і потребує окремого математичного моделювання, H_i -параметри Ляме (i= 1, 2, 3), точкою позначені похідні за часом, α^i – ортогональні криволінійні координати

$$W_\bullet=S_{ij}\dot{Э}_{ij}-\frac{1}{2G}S_{ij}\dot{S}_{ij}+\frac{\sigma_{ii}}{3}\left(\dot{\varepsilon}_{jj}-3\alpha_T\frac{\partial T}{\partial t}\right)-\frac{\sigma_{ii}}{3K}\dot{\sigma}_{jj},$$

$$S_{ij}=\sigma_{ij}-\delta_{ij}\sigma,\qquad Э_{ij}=\varepsilon_{ij}-\delta_{ij}\varepsilon, \qquad (2)$$

$$\sigma=\frac{\sigma_{ii}}{3},\quad \varepsilon=\frac{\varepsilon_{ii}}{3},\ G=\frac{E}{2(1+\nu)},\ K=\frac{3E}{1-2\nu}.$$

Де S_{ij} ,$Э_{ij}$ - відповідно девіатори тензорів напруг і деформацій, σ_{ij} ,ε_{ij} - тензори напруги і деформації.

Початковий розподіл температури в тілі, що відповідає природному ненапруженому стану тіла, задається так

$$T=T_0(\alpha^i)\qquad \text{при}\qquad t=0. \qquad (3)$$

Граничні умови, які відображають вплив навколишнього середовища на температуру тіла, задаються в такий спосіб

$$\lambda\cdot\frac{\partial T}{\partial n}=-\alpha(T-\theta)-q, \qquad (4)$$

де n - зовнішня нормаль до поверхні тіла, α_T - коефіцієнт лінійного теплового розширення, α - коефіцієнт теплообміну, Θ - температура навколишнього середовища, q - тепловий потік.

У загальному випадку величини α, Θ, q можуть залежати від часу й положення точки (α^1, α^2, α^3) на поверхні тривимірного тіла V. Умова (4) при різних значеннях коефіцієнта α містить три види граничних умов. Граничні умови першого роду полягають у тому, що на поверхні тіла в кожний момент часу заданий розподіл температури ($\alpha\to\infty,\ q=0$). Граничні умови другого роду задають тепловий потік q через поверхню тіла ($\alpha=0,\ q\neq0$). Граничні умови третього роду формулюють закон теплообміну між поверхнею тіла й навколишнім середовищем при заданій величині $\Theta(q=0,\ \alpha\neq0)$ [1].

Окрім температури в кожній точці тіла треба знайти зміщення точок тіла u_i (або їх

швидкості v_i) і тензори напруги та деформації.

Для створення повної математичної моделі поведінки пружно-пластичних циліндричних тіл під дією температурного та силового навантаження необхідно більш детально розглянути: геометричні співвідношення та рівняння руху елемента пружно-пластичного циліндричного тіла, моделі фізичних співвідношень термопружності та термопластичності [2].

Повну систему рівнянь запропонованої моделі можна записано в векторній формі [1,2]

$$\frac{\partial \vec{W}}{\partial t} = \sum_{i=1}^{2} A_i \frac{\partial \vec{W}}{\partial \alpha_i} + \vec{B}, \qquad (5)$$

де $\vec{W}$- вектор, компонентами якого будуть швидкості зміщень, компоненти тензорів напруги та деформації. Така форма представлення моделі пружно-пластичного циліндричного тіла дає можливість подальшого її дослідження різними чисельними методами, наприклад: метод скінчених різниць, метод кінцевих елементів. Дослідження останніх років свідчать про те, що перспективними методами для моделювання поведінки пружно-пластичних тіл під дією температурних та силових навантажень є методи розщеплення і сплайн-колокації, які дозволяють будувати точніші розв'язки, як за часом, так і по координатах [5].

Таким чином, тривимірне рівняння теплопровідності (1), з урахуванням пружних параметрів, які залежать від температури разом з початковими умовами (3) і граничними умовами (4) дозволяють визначити неосесиметричне температурне поле в циліндричному тілі [3,4], і бути представлене у векторній формі (5). Реалізація моделювання пружно-пластичних циліндричних тіл, з урахуванням пружних параметрів, які залежать від температури, можлива за допомогою інструментальних засобів комп'ютерного моделювання ABAQUS, ANSYS, які базуються на основі методу кінцевих елементів.

Список літератури

1. Стеблянко П.А. Пространственные нестационарные задачи теории термоупругопластичности. НАН Украины, Институт механики, Министерство образования Украины, ДГТУ. 1997. – 273с.

2. Pavel A. Steblyanko, Konstantin E. Dyomichev. Application of Fractional Steps Method for Determining the Stress and Strain Field during the Temperature Load of Cylindrical Bodies. // DOI 10.12851/EESJ201501C06ART06. Eastern European Scientific Journal. ISSN 2199-7977 Ausgabe 1-2015, p. 138 -147.

3. Стеблянко П.О., Дьомічев К.Е. Моделювання поля напруження та деформації при нестаціонарному температурному навантаженні циліндричних тіл // «Строительство, материаловедение, машиностроение» Серия «Энергетика, экология, компютерные технологи в строительстве. - Випуск 76.- Днепропетровськ, 2014- С.262-270.

4. Дьомічев К.Е. Моделювання поведінки температурних навантажень для деяких деталей машин, які працюють в умовах підвищених температур. Тези доповідей IV Міжнародної науково – практичної конференції «Актуальні наукові дослідження в сучасному світі», Переяслав - Хмельницький, 2015.-с.136-140.

5. Стеблянко П.А., Волосова Н.Н., Дьомічев К.Е. Застосування методу дробових кроків для визначення поля напруження та деформації при температурному навантаженні циліндричних тіл. Математичні проблеми технічної механіки. Збірник наукових праць Дніпродзержинського державного технічного університету. Тематичний випуск. - Випуск 2(19).- Дніпродзержинськ, 2012.- С. 78-85.

УДК 004.735

Тенденции развития услуг в условиях внедрения сетей 3G

Игнатьева В.Ю., бакалавр, Vikyllia@bigmir.net
Научный руководитель – Ступак Г.В., ст. преп. каф. АТ
Донецкий национальный технический университет, г. Красноармейск

Мобильный широкополосный доступ в Интернет сегодня в Украине становится все более популярным. Старт широкомасштабного внедрения услуг 3-го поколения мобильной связи в 2015 году позволяет вывести на рынок услуг значительное количество новых и востребованных сервисов. На сегодняшний день карта покрытия «чистым 3G» не достаточно обширная по территории, но значительна по величине абонентской базы (охват менее 10% территории, количество абонентов порядка 20 млн.) [1]. По результатам исследований компании AC&M в 2015 году количество активных пользователей в сетях операторов Украины достигло 59,45 млн., распределение абонентской базы следующее: Київстар – 26,158 млн.аб., Vodafone – 20,213 млн.аб., Lifecell – 10,701 млн.аб., другие – 2,378 млн.аб.[2].

С точки зрения предоставляемых услуг до 2015 года, доминирующими были услуги классической телефонии, передачи сообщений и услуга пакетной передачи GPRS/EDGE, что в первую очередь связано с технологией существующих сетей – 2G. Внедрение 3G позволяет существенно расширить спектр услуг пакетной передачи данных. Как показывают исследования [3], изменились не только объемы используемого трафика, но и предпочтения в выборе контента. Так, потребление постепенно смещается в сторону более «тяжелых» видов трафика, таких как видео-контент и аудио. В процентном соотношении прирост объема данного трафика практически удвоился в сети 3G в сравнении с 2G, также внедряются новые услуги, которые используют облачные технологии.

Не последнюю роль играет и тот факт, что доля смартфонов и планшетов на рынке стремительно растет по сравнению с обычными телефонами. Анализируя статистику последних лет, доля «умных» устройств увеличилась с 10% в 2013 до 59% в 2015 году [4].

Исходя из изменений на рынке устройств и переходу на новые технологические стандарты, необходимо внедрение перспективных услуг, которые были бы востребованы пользователями. Для расстановки приоритетов в развитии мобильных услуг, студентами и сотрудниками кафедры АТ ДонНТУ запущен сервис по анкетированию [5] (сервис актуален и продолжает работу). Вопросы анкеты сгруппированы по таким тематическим секциям:

– общая информация: возраст, географическая принадлежность, онлайн-сервисы которые использует респондент, тип операционной системы:

– использование памяти смартфона: фото, музыка, видео и используются ли респондентом облачные хранилища;

– использование смартфона не по прямому назначению: видеонаблюдение, умный дом, мобильный офис;

– экономия на услугах связи при помощи смартфона: как часто осуществляются звонки за границу, уровень использования приложений IP-телефонии.

На текущий момент в опросе приняло участие 475 человек (с 23.02.2016 по 05.03.2016), с общим количество респондентов 475 и полным охватом территории Украины. Основные результаты обработки ответов респондентов представлены в таблице 1.

Исходя из полученных текущих результатов анкетирования, доминирующая операционная система – Android; степень использования онлайн сервисов высокая, причем лидируют социальные сети, аудио- и видео-онлайн; большая часть респондентов испытывает проблемы с нехваткой свободного места на устройстве, причем хранения фото и аудио приоритетнее, чем хранение видео; более половины респондентов используют облачные хранилища, хотя есть и такие, кто не знает что это; респонденты активно используют сервисы IP-телефонии для экономии расходов на звонки за границу; проявляют интерес к концептуально новым и не получившим пока распространения услугам таким как удаленное видеонаблюдение, умный дом и мобильный офис.

Таблица 1 – Текущие результаты анкетирования

Общая информация		Тип ОС		Использование облачного хранилища	
Возраст		Android	76,4	Да	58,5
0-16	2,1	Apple iOS	13,8	Нет	31,2
17-22	50,5	Windows Phone	5,3	Я не знаю что это	10,3
23-27	18,9	Blackberry	0,4	Экономия на услугах связи	
28-35	18,1	Другая	4,1	Звонки за границу	
36-55	9,5	Память смартфона		Каждый день	3,8
55+	0,8	Нехватка места		Через день	3,4
География		Да	60	1 раз в неделю	10
Центр Украины	10,3	Нет	40	1 раз в месяц	17,5
Юг Украины	3	Фото		Не пользуюсь	65,3
Север Украины	3,9	0-30%	56,6	Приложения IP-телефонии	
Восток Украины	80,8	31-50%	28,2	Да	89,7
Запад Украины	2	51-70%	11,8	Нет	10,3
Онлайн-севрисы		70+%	3,4	Использование смартфона не по назначению	
Онлайн аудио	64,3	Музыка		Видео наблюдение	
Онлайн видео	65,5	0-30%	58,5	Да	73,3
Социальные сети	92,6	31-50%	26,9	Нет	26,7
Онлайн игры	25,2	51-70%	8,8	Умный дом	
Умный дом	3,2	70+%	5,8	Да	74,5
Мобильный офис	34,9	Видео		Нет	25,5
Обл. хранилище	41	0-30%	90,9	Мобильный офис	
Видеонаблюдение	5,1	31-50%	6,3	Да	57,5
Новостная лента	61,1	51-70%	1,9	Нет	19,2
Другое	6,3	70+%	0,9	Я не знаю что это	23,4

Основываясь на проведенном анализе предметной области и текущих результатах анкетирования, можно сделать следующие выводы:

– уровень покрытия 3G в Украине растет;

– количество зарегистрированных абонентов практически достигло своего максимума (на одного жителя Украины в среднем приходится 2 номера), что связано с соизмеримыми тарифами ведущих операторов;

– структура трафика мобильной сети неуклонно стремится к «пакетизации» и «утяжелению», и все более смещаются акценты в сторону передачи пакетных данных в высокоскоростных сетях широкополосного абонентского доступа;

– текущие результаты проводимого анкетирования свидетельствуют о нехватке места на устройствах и потребности абонента в концептуально новых услугах, которые позволят использовать смартфон не только как «модный гаджет», но и как инструмент мониторинга в системе безопасности или же, как средство управления домом либо каким другим объектом.

Дальнейшая работа будет направлена на разработку мобильных приложений, которые позволят найти применение для смартфона не только как телефона, но и как инструмента.

Список литературы:

1. Зведена карта покриття всіх 3G GSM операторів України [Электронный ресурс] – Режим доступа: http://3g.multitest.ua/?pos=47.20108,33.74311,7

2. Число абонентов мобильной связи в Украине составило 59,45 млн [Электронный ресурс]. – Режим доступа: http://tapker.com/news/cislo-abonentov-mobilnoj-svyazi-v-ukraine-sostavilo-5945-mln_p133.html

3. Запуск 3G в сети Vodafone изменил не только объем, но и характер потребления интернет-трафика [Электронный ресурс]. – Режим доступа: http://itc.ua/news/zapusk-3g-v-seti-vodafone-izmenil-ne-tolko-obem-no-i-harakter-potrebleniya-internet-trafika/

4. Продажи мобильных телефонов в Украине просядут на 20-30%. При этом продолжит увеличиваться доля смартфонов [Электронный ресурс]. – Режим доступа: http://business.vesti-ukr.com/94367-prodazhi-mobilnyh-telefonov-v-ukraine-prosjadut-na-20-30

5. Соцопрос: Насколько Вы используете возможности Вашего смартфона? [Электронный ресурс]. – Режим доступа: https://goo.gl/SF9nVa

УДК 004.9

Киберспорт – бизнес будущего

Кожокару Н.Р., студент IV курса, nikitakozokaru@gmail.com
Научный руководитель – Охрименко С.А., д.э.н., профессор
Молдавская Экономическая Академия, Кишинёв, Молдова

Введение

На сегодняшний день, зачастую, слово *«киберспорт», не воспринимается всерьез. Тем не менее игровой бум, совпавший с началом третьего тысячелетия, способствовал формированию огромного киберспортивного рынка, который тесно связан с другими смежными отраслями информационного бизнеса [1]*.

Киберспорт представляет собой соревнования, в которых используются компьютерные, информационные и коммуникационные технологии. На основе программных компонентов и графических приложений компьютер моделирует виртуальное пространство, внутри которого происходит состязание. Все компьютерные игры и соревнования по ним, делятся на несколько основных классов, различаемых свойствами пространств, моделей, игровой задачей и развиваемыми игровыми навыками кибер-спортсменов [7].

Не стоит забывать, что свои корни киберспорт берёт из специализированных программ обучения и виртуальных тренажёров, так называемых симуляторов, имитирующих управление каким-либо процессом, аппаратом или транспортным средством. Со временем тенденция сменила направление. Теперь развитие киберспорта и совершенствование игрового процесса способствует появлению новых высокоразвитых и продуманных до мельчайших подробностей симуляторов.

Несмотря на то, что ведущие производители и известные брэнды спонсировали соревнования последние 15 лет, призовые были не очень велики, от нескольких тысяч, до нескольких десятков тысяч долларов на дисциплину. И это был общий призовой фонд, а не приз за первое место. Еще чаще игроки становились жертвами собственных менеджеров, которые присваивали львиную долю призовых себе за «организацию». Зарабатывать на жизнь в этой сфере было невозможно, приличные деньги получали единицы.

Все изменилось в последние несколько лет, когда команда justin.tv в июне 2011 года запустила сервис Twitch.tv. В настоящее время данный ресурс является ведущим сайтом потокового видео, где основная тема вещания — игровое видео и прямая трансляция киберспортивных турниров. Благодаря сочетанию технических средств, программного обеспечения, развитых коммуникаций и маркетинговой компании, в киберспорт наконец-то пришли крупные деньги. Когда производители аксессуаров и оборудования увидели, что трансляции смотрит 10-15 тысяч человек одной языковой группы, они начали активно рекламировать свою продукцию, а также спонсировать всевозможные лиги и турниры. На данный момент игровые трансляции смотрят сотни тысяч человек по всему миру [2].

Например, киберспорт в Корее развит как нигде в мире. Фанаты стараются собираться вместе для просмотра матчей любимых команд. Специализированные площадки площадки постоянно заполнены посетителями до отказа. Из-за невероятной популярности электронных игр и огромных успехов корейских профессионалов в различных видах киберспорта фанаты из других стран смотрят на Корею как на киберспортивный рай. Это страна, в которой к профессиональным киберспортсменам относятся так же уважительно, как к звездам мирового футбола [8].

Тем не менее, киберспортивные соревнования способствуют не только популяризации компьютерных игр и увеличению аудитории. Киберспорт, предоставляет благоприятную почву развитию новых технологий, таких как очки виртуальной реальности, новые гаджеты и специализированное программное обеспечение, а также является перспективным бизнесом. В рынок только начинают вкладываться большие деньги и общий прогноз предполагает его

взрывной рост к 2020 году. Киберспорт становится явлением мирового масштаба. И игнорирование этой рыночной ниши с точки зрения бизнеса по меньшей мере недальновидно.

Маркетинговая компания NewZoo, специализирующаяся на исследованиях игровых рынков, в своём отчёте о глобальном росте киберспорта предсказывает огромный рост прибыли. Для сравнения в 2014 году общий годовой доход в этой области составлял 194 $миллионов, а по прогнозам NewZoo, к 2017 году доход возрастёт до 465 $миллионов.

Двадцать лет назад, идея введения Экстремальных видов спорта на Олимпиаде казалась фантастической. Сегодня развитие такого спорта неизбежно. Так что, возможно, не так нелепо слышать высказывания Брэндона Бека, генерального директора Riot Games, о том, что киберспорт станет частью Олимпийских игр еще при его жизни.

Заключение

У всего есть свои достоинства и недостатки и киберспорт не является исключением. Данная сфера доступна, предоставляет широкий ряд новых профессий, таких, как репортёры, менеджеры, экономисты, а также довольно перспективна, как в экономическом, так и технологическом плане. С другой стороны, кибероспорт негативно влияет на здоровье, отбирает много времени и сил. Киберспорт способствует развитию информационных технологий, что с одной стороны ускоряет прогресс и дарит человечеству новые технологии, но с другой стороны виртуальная реальность отдаляет людей от реального общения и восприятия мира, а развитие киберспорта, как нового витка в бизнес индустрии способствует появлению новых угроз информационной безопасности. Поскольку киберспорт базируется на моделировании и анализе современных технических устройств, эта среда может послужить основой для отработки новых методов и средств нападения. Самое страшное, заключается в том, что, имея огромную аудиторию и собственные СМИ, кибеспорт не только может стать новым пунктом в списке угроз информационной безопасности, но и превратиться в одно из самых эффективных орудий информационного терроризма.

Литература

1. Шаталов Н., "Киберспорт: бизнес, который захватит мир // "http://www.tpp-inform.ru/analytic_journal/6674.html// 03 марта 2016

2. "Противоречие последних лет или киберспорт как новое явление в индустрии развлечений" // https://habrahabr.ru/post/228201// 1 июля 2014

3. Белова И., "Как и почему растет индустрия киберспорта"// https://vc.ru/p/the-next-ten-years-of-esports// 04 января 2016

4. Савин С., "Киберспорт - как бизнес-тренд будущего"// http://www.cossa.ru/155/102730// 15 мая 2015

5. "Как все устроено. Киберспорт"// http://www.eurosport.ru/e-sports/story_sto4815699.shtml// 10 июля 2015

6. Heitner.D., "The Business of eSports Is On Pace To Explode"// http://www.forbes.com/sites/darrenheitner/2015/10/15/the-business-of-esports-is-on-pace-to-explode/#7cdecc1e6d87// oct. 2015

7. "Киберспорт"// https://ru.wikipedia.org/wiki/киберспорт

8. "Киберспортивная Корея"// http://ru.leagueoflegends.com/ru/news/esports/esports-editorial/kibersportivnaya-koreya//

9. "The Global Growth of Esports"//https://images.eurogamer.net/2014/dan.pearson/Newzoo_Preview_Images_Global_Growth_of_Esports_Report_V4.pdf// 2014

10. Laximisha R., Gao Y, "Future Perspectives on Next Generation e-Sports Infrastructure and Exploring Their Benefits"//http://www.worldacademicunion.com/journal/SSCI/sscivol03no01paper05.pdf// 2009

УДК 004.056.53

Огляд додатків доповненої реальності

Колісніченко О.Ю., студент 3 курсу, CoolMeLater@ya.ru
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Сьогодні ми живемо в світі новітніх технологій, більшість із яких вражає своєю футуристичністю, і все ближчає той день, коли те, що ми вважали науковою фантастикою, стане реальністю. Однією із таких технологій є доповнена реальність – технологія, яка буквально змінить наш світогляд.

Доповнена реальність (із англійського «augmented reality», або AR) – це загальний термін, який використовується до усіх розробок та проектів, які використовують віртуальні технології для «доповнення» реального оточення. Доповнена реальність – це частина «змішаної реальності», в яку також входить «доповнена віртуальність» (це навпаки, коли реальні об'єкти інтегруються у віртуальне середовище).

Найпростіші приклади AR ми бачимо щоденно: візуальні інформаційні ефекти на телетрансляціях, а саме траєкторія м’яча під час матчу, дані про відстань між двома об’єктами, і таке інше. Також до цих технологій відносяться сучасні навігатори і інтерактивні мапи в авто та літаках.

Сам термін доповненої реальності був створений під час співпраці Тома Кодела з корпорацією Boeing дослідником в 1990 році. Дослідник Рональд Азума в 1997 році започаткував визначення доповненої реальності як системи, яка:

– Поєднує віртуальне і реальне.
– Взаємодіє у реальному часі.
– Працює в 3D.

Іноді доповнену реальність також називають розширеною, поліпшеною, або збагаченою реальністю.

Також, зараз розроблюється багато різноманітних, на рівень складніших проектів у цій область, які для багатьох раніше виглядали, як наукова фантастика.

Нижче представлено приклад роботи такого проекту – «Wikitude World Browser» на iPhone 3GS, що використовує GPS і цифровий компас для відображення доповненої реальності:

Рисунок 1 – Wikitude World Browser наiPhone 3GS

Крім простих проектів із «доповненими» інтерфейсами, зараз розробляються і деякі, неймовірно складні продукти, які можуть, буквально, змінити точку зору людства щодо багатьох речей.

Прикладом таких проектів є розроблені корпорацією «Google» спеціальні лінзи для діабетиків. Ці лінзи мають спеціальну вбудовану систему, яка аналізує склад сліз людини, і з'ясовує таким чином рівень цукру, після чого виводить відповідну інформацію на будь-який пристрій користувача на базі ОС android.

Рисунок 2 – «Розумні» лінзи для діабетиків від Google

Окрім вже наявних функцій, «Google» вже працює над тим, щоб додати до цих лінз спеціальну функцію для постійного відображення даних про рівень цукру прямо на лінзі.

Також, використовуючи експериментальні лінзи із технологією «Eyecatch», корпорація «Google» хоче доповнити свій вже існуючий продукт – «Google Glasses», додавши можливість контролю інтерфейсу напрямком зору людини. Ця технологія вже виглядає як щось із науково-фантастичного фільму, але це реальність, яку ми можемо побачити в магазинах вже у найближчі два-три роки.

Висновок: Отже, сучасні технологічні можливості дозволяють не тільки розвивати саму технологію AR, але й використовувати її в повсякденному житті. Доповнена реальність має безліч різноманітних способів і шляхів застосування й до того ж є неймовірно зручною, тому є дуже перспективним її розвивати й надалі, щоб поліпшити вимоги до її використання й розширити її функціонал, а як результат – і користь від неї.

Список літератури

1. Доповнена реальність і віртуальність [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/

2. Технології доповненої реальності [Електронний ресурс]. – Режим доступу: http://www.softline.kiev.ua/ua/soft-na-zamovlennya/tekhnologiji-dopovnenoji-realnosti.html

УДК 004.716

Обмеження задач оптимізації розподілу пропускних здатностей систем гетерогенних інфокомунікаційних мереж

Ладигіна О.А., ladyginaoa@ukr.net
Кіровоградський національний технічний університет, м. Кіровоград

Оптимізація інформаційно-обчислювальних мереж на мережевому рівні як наукове завдання існує достатньо давно. Проте, традиційні підходи, коли мережі представляються як одноканальні, багатоканальні системи масового обслуговування або у вигляді зв'язних графів накладають певні обмеження на область застосування отриманих результатів[1].

Так штучне розчленовування мережі на ряд незалежних ланок веде до істотних погрішностей обчислень при аналізі мережі як єдиної структури. Крім того, відмова від урахування специфіки побудови окремих каналів зв'язку приводить до невиправданого загрубіння моделей і, як наслідок, встає питання про відповідність результатів, одержаних за допомогою таких моделей, реальній поведінці мережі. Питання статистичного ущільнення і методика розрахунку допустимої кількості віртуальних з'єднань різних служб в цифровому тракті, залежно від кількості джерел і параметрів трафіку при заданих значеннях параметрів якості обслуговування, є цікавим самостійним завданням, пов'язаним з управлінням ресурсами.

Тому актуальним є побудова математичних статистичних моделей глобальних критеріїв оптимальності обслуговування трафіку в гетерогенних інфокомунікаційних мереж, що включають системи, лінії зв’язку з різними принципами дії та техніко-економічними характеристиками, пошук розподілу оптимальних пропускних здатностей ліній зв’язку з урахуванням їх особливостей і реально існуючих обмежень на умови розв’язання задач оптимізації.

Основним методом розв’язання задач оптимізації є метод невизначених множників Лагранжа, який дозволяє розв’язувати нелінійні задачі математичного програмування і врахувати обмеження на допустимі значення керованих змінних [2]. Логічний смисл допоміжного множника Лагранжа полягає в тому, що він коригує мінімальні значення математичного сподівання сумарних витрат на функціонування *N*-системи інфокомунікаційної мережі в залежності від параметрів, вагових коефіцієнтів, а також керованих змінних.

Розв’язання задач різних класів вимагає різних вхідних даних. Наприклад, деякі задачі певних класів потребують знання коефіцієнтів варіації тривалості обслуговування, а також попереднього розв’язання одномірної задачі оптимізації для *i*-ої системи. Тому використання різних за змістом вагових коефіцієнтів q_i в математичній моделі критерію оптимальності (1) дозволяє враховувати не менше п’яти принципових різниць в техніко-економічних характеристиках систем гетерогенних інфокомунікаційних мереж або видів їх трафіку [3].

$$D_N(q_i, n_i, N_s, a_i, b_i, C_i) = \sum_{i=1}^{Ns} q_i D_i = \sum_{i=1}^{Ns} q_i \left(P_i(n_i \geq N_i) a_i c_i^{-1} + P_i(n_i < N_i) b_i c_i \right), \qquad (1)$$

де N_s – загальне число різнорідних систем обслуговування трафіку в гетерогенній інфокомунікаційній мережі, $i = 1, N_s$;

D_i – локальний критерій оптимізації для *i*-ої системи;

a_i і b_i - випадкові параметри функцій втрат і витрат в *i*-ої системи;

C_i - пропускна здатність вихідної *i*-ої канальній лінії зв’язку;

$P_i(n_i \geq N_i)$ і $P_i(n_i < N_i)$ - ймовірності того, що лінія буде зайнята або вільна.

Для зручності розв’язання задач різних класів проведена класифікація техніко-економічних характеристик:

1. Лінії відрізняються витратами, що обумовлені відмовами в обслуговуванні повідомлень.
2. Лінії відрізняються витратами на одиницю пропускної здатності лінії.
3. Лінії відрізняються середніми коефіцієнтами використання пропускної здатності.

4. Лінії відрізняються коефіцієнтами варіації тривалості обслуговування повідомлень, тобто затримками в черзі повідомлень

5. Лінії відрізняються максимальними значеннями математичного сподівання сумарних витрат.

Для реально існуючих обмежень на умови розв'язання задач оптимізації також можна виконувати класифікацію за певними ознаками, що подібна наведеної. Для цього зручно представити обмеження в такому узагальненому вигляді:

$$C_N = \sum_{i=1}^{N} g_i C_i, \qquad (2)$$

де вагові коефіцієнти g_i, $i = 1, N,$ обираються в залежності від реально діючого класу обмеження.

Найбільш суттєві класи обмежень:

1. Всі коефіцієнти однакові, тоді обмеження накладається на загальну сумарну пропускну здатність усіх систем інфокомукаційної мережі.

2. Обмеження накладається на загальну щорічну вартість обслуговування систем мережі.

3. Обмеження враховує витрати, що обумовлені відмовами в обслуговуванні пакетів даних в мережі.

4. Обмеження враховує витрати на одиницю пропускної здатності системи.

5. Обмеження враховує коефіцієнти варіації тривалості обслуговування.

6. Обмеження враховує максимальні значення математичного сподівання сумарних витрат.

Обидві класифікації не є вичерпними, наприклад, якщо необхідно враховувати пріоритети трафіку по каналах, тоді треба обирати вагові коефіцієнти на основі рангів трафіків. Крім цього, може діяти не одне, а декілька обмежень. Наприклад, може бути одночасно два обмеження, коли обмеження накладається на загальну сумарну пропускну здатність усіх систем інфокомукаційної мережі і на загальну щорічну вартість обслуговування систем мережі.

Головна вимога для задач оптимізації з обмеженнями: загальне число m_l обмежень не повинно дорівнюватися або бути більше числа керованих змінних, тобто повинна виконуватися необхідна умова:

$$m_l \le n_c, \left(m_l / n_c\right) \le 1 \qquad (3)$$

де n_c – загальне число керованих змінних.

При виконанні умови (3) оптимальне рішення існує і є однозначним.

Висновки. Отримана класифікація обмежень задач оптимізації за ознаками вибору значення вагових коефіцієнтів може служити основою для обґрунтування обмеження в прямій постановці задачі оптимізації розподілу реалізацій пропускних здатностей систем гетерогенних інфокомунікаційних мереж. Тому що найбільш важливим є точне визначення виду критерію оптимальності і діючих обмежень оптимізації, що визначають клас задачі оптимізації. Врахування класу задачі дозволяє бути впевненим, що вирішується саме та задача оптимізації обслуговування трафіку, яка є актуальною для зменшення середнього ризику.

Список літератури

1. Ладигіна О.А. Дослідження методів та моделей управління трафіком в комп'ютерних мережах //Проблеми інформатизації та управління: Збірник наукових праць: Випуск 4 (36). – К.: НАУ, 2011. – С.60-66.

2. Методи аналізу трафіку гетерогенних комп'ютерних мереж [Текст] : автореф. дис. . канд. техн. наук : 05.13.13 / Г. В. Даниліна ; Національний авіаційний університет. - К., 2007. - 20 с.

3. Ігнатов В.О., Гузій М.М, Ладигіна О.А. Статистична оптимізація обслуговування трафіка в гетерогенних інфокомунікаційних мережах //Проблеми інформатизації та управління: Збірник наукових праць: Випуск 1 (49). – К.: НАУ, 2015. – С.37-40

УДК 004.942: 656.021

Модель інтелектуальної системи управління міським пасажирським автотранспортом

Лахно В.А., д.т.н., доцент, Valss21@ukr.net,
Собченко В.М., аспірант, floydrose@i.ua
Європейський університет, м. Київ

Вступ. Міський пасажирський автотранспортний комплекс утворюють сукупність автобусів та маршрутних таксі, управляючий ними персонал та вся інфраструктура, яка визначає ефективність його функціонування. Сучасні комп'ютерні системи диспетчерського управління міським пасажирським автотранспортом (СДУМАТ) базуються на використанні наукомістких технологій, затребуваних необхідністю підвищення ефективності управління дорожнім рухом, зокрема у великих містах.

Основна задача СДУМАТ – задоволення потреби пасажирів у поїздках. Вона вирішується за рахунок виконання розкладу, а також підключення у випадку необхідності резервних транспортних засобів.

Модель. Для підвищення ефективності СДУМАТ, розроблено модель з урахуванням впливу найбільш значущих стохастичних чинників, яка описується системою рівнянь:

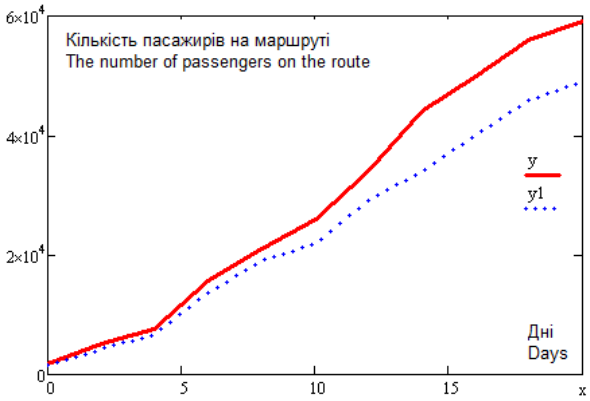
$$
\left.
\begin{aligned}
& t_i^1 = t_i^{нчр(k)}; \\
& Q_i^0 = 0; \\
& .q_i^1 = 0; \\
& \nu_i^j = \frac{i}{n}\eta_i \rho^j(t); \\
& q_i^j = \nu_i^j Q_i^{j-1}; \\
& r_i^j = A_i - (Q_i^{j-1} - q_i^j); \\
& P_i^j = \int_{t_{i-1}^j}^{t_i^j} \rho^j(t)dt; \\
& d_i^j = P_i^j + g_{i-1}^j; \\
& Q_i^j = \min\left\{A_i, A_i + d_i^j - r_i^j\right\}; \\
& g_i^j = \max\left\{0, d_i^j - r_i^j\right\}; \\
& \tilde{P}_i^j = d_i^j - g_i^j; \\
& q_i^n = Q_i^{n-1}; \\
& P_i^n = 0; \\
& \tau_{ні}^j = \eta_i(\tilde{P}_i^j + q_i^j); \\
& \tau_{зі}^j = \tau_з(U); \\
& \tau_i^j = \begin{cases} \tau_{ні}^j, \text{if } \tau_{зі}^j \le \tau_{ні}^j, \\ \tau_{зі}^j, \text{if } \tau_{зі}^j > \tau_{ні}^j; \end{cases} \\
& v_i^j = v(U); \\
& \tilde{\tau}_i^{j+1} = l^j / v_i^j; \\
& t_i^{j+1} = t_i^j + \tilde{\tau}_i^{j+1} + \tau_i^j; \\
& \tau_i'^j = t_i^j - t_{i-1}^j.
\end{aligned}
\right\}
$$

$$
i = \overline{1,m};\ \ j = \overline{1,n},
$$

де m – кількість рухомих одиниць (РО); n – кількість пунктів зупинки (ПЗ); l^j – відстань між j-м та $j+1$-м ПЗ; $t_i^{нчр(k)}$ – час початку k-го рейсу; A_i – місткість i-ї РО; $v(U)$ – випадкова величина, яка характеризується законом розподілу швидкості руху при даній ознаці управління; $\tau_з(U)$ – випадкова величина, яка визначає час затримки як функцію від ознаки управління; η_i – випадкова величина, яка характеризує інтенсивність посадки та висадки для i-ї РО; ν_i^j – випадкова величина, яка характеризує кількість пасажирів, що виходять з i-ї РО на j-му ПЗ; $\rho^j(t)$ – випадкова величина, яка характеризує щільність пасажиропотоку на j-му ПЗ; t_i^j – час прибуття РО на j-й ПЗ; Q_i^j – наповнення i-ї РО після обслуговування j-го ПЗ; $\tilde{\tau}_i^{j+1}$ – час, затрачений на рух по перегону маршруту між j-м та $j+1$-м ПЗ; $\tau_{ні}^j$ – час, який витрачається на посадку та висадку пасажирів на j-му ПЗ i-й РО; $\tau_i'^j$ – час руху між $i-1$-ю та i-ю РО після проходження j-го ПЗ; $\tilde{P}_i^j$, q_i^j – кількість пасажирів що зайшли та вийшли, відповідно; $v(U)$ – випадкова величина, що характеризується законом розподілу швидкості руху при даній ознаці управління; P_i^j – кількість пасажирів, що прийшли до j-го ПЗ за час між прибуттям i-ї та $i-1$-ї РО; r_i^j – резерв місць в i-й РО на j-му ПЗ; g_i^j – кількість не обслужених пасажирів i-ю РО j-м ПЗ; d_i^j – потреба в перевезенні з j-го ПЗ в момент прибуття i-й РО.

Критерієм якості задоволення потреб в поїздках являється мінімізація часу очікування пасажирами транспорту. Всі порушення руху транспорту – відхилення від розкладу, переповнення, які являються наслідком нерівномірної швидкості руху окремих рухомих одиниць та флуктуацій пасажиропотоку, викликають збільшення часу очікування. Тому і ефективність управляючих дій має сенс оцінювати по тому ж критерію.

Результати. Запропонована в статті модель реалізована в MathCAD. Результати моделювання наведені на рис. 1.



y —— – використання моделі СДУМАТ;
y1 ····· – без використовування моделі

Рисунок 1 – Результати моделювання СДУМАТ в Mathcad

Впровадження одержаних результатів досліджень дало можливість значно підвищити якість транспортного обслуговування, зокрема на автобусних маршрутах № 203 та № 510 м. Києва.

Економічний ефект склав 3730 та 4500 грн. на місяць, продуктивність маршрутів зросла на 7,1% та 8,3%, відповідно.

Висновки. Запропонована математична модель являється працездатною та дозволяє адекватно описувати процес руху рухомої одиниці по маршруту. Використання пакету Mathcad в реальній практиці експлуатації СДУМАТ не є можливим, оскільки його застосування передбачає певну кваліфікацію користувача, отже подальша робота планується в напрямку розробки відповідного програмного продукту.

УДК 004.4'2

Використання front-end технологій для розробки презентацій

Майоров Є.О., студент 2 курсу, hitstalker@rambler.ru
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Серед способів розповсюдження інформації в навчальному або робочому процесі одним з найефективніших є використання презентацій. Зазвичай вони створюються за допомогою програм Microsoft PowerPoint або Keynote.

Цей спосіб має два недоліки:

1.Створення, перегляд і подальше редагування презентації повинні виконуватися тільки цими програмами, що призводить до повної залежності від цих програм і відповідних ОС для Microsoft PowerPoint – це Windows, для Keynote – Apple.

2.Завдяки великій кількості «готових» презентацій, шаблонність створення, структури, загального вигляду презентації – це явище масове, що негативно відображається на креативності і оригінальності самих презентацій.

Ці недоліки змушують звернутися до альтернативних варіантів.

Одним з альтернативних варіантів створення презентацій є використання синтезу HTML5, CSS3 і JavaScript, де присутність JavaScript в лістингу варіюється від декількох скриптів до охоплення всієї функціональної частини (JavaScript-фреймворки).

Перевагами використання синтезу HTML5, CSS3 і JavaScript є:

1.Можливість створення презентації без прив’язування до конкретного ПЗ або ОС: є безліч середовищ розробки, офлайн- і онлайн-редакторів лістингу для ОС Windows, *nix або OS X.

2.Можливість «творчого» створення презентації. Різноманітність інструментів (теги, класи і т.д.) в HTML5, CSS3 разом з можливостями JavaScript набагато вища, ніж в Microsoft PowerPoint або Keynote

3.Завдяки front-endовій природі презентації можливість редагування презентації не прив’язана до програми створення презентації: наприклад, лістинг презентації можна редагувати навіть у самому браузері.

Але є і недоліки:

1.Семантика HTML5, CSS3 і JavaScript, не кажучи про особливості цих технологій, вимагають деяких зусиль і часу для їх вивчення і використання. Це особливо актуально для «непрограмістів».

2.Створення презентації «з нуля» охоплює безліч аспектів: від створення базового каркасу презентації до інтеграції CSS-бібліотек або JS-фрейворків, окремих «features».

3.Інколи для відображення складних або недавно створених елементів, функцій, анімацій, ефектів HTML5 і CSS3 необхідні сучасні браузери, і навіть вони інколи не здатні забезпечити коректність зображення.

Вдалими прикладами використання синтезу HTML5, CSS3 і JavaScript є наступні:

1. CSS-based SlideShow System – CSS-фреймворк для створення презентацій з використанням сучасних веб-стандартів, створенний Lea Verou для Front Trends 2010. Особливостями даного CSS-фреймворку є:

- Особлива увага при створенні файлової структури презентації приділяється CSS-файлам.
- Для маніпуляції параметрами слайдів (довжина, висота) використовуються em.
- Реалізована навігація презентації за допомогою клавіатури.
- Реалізований плагін, що дозволяє описувати лістингом не до кінця стандартизовані властивості CSS3 без «vendor prefixes».
- Реалізований плагін для освітлення програмного коду, записаного в тегу <code>.

2. DZSlides – HTML-файл для створення презентацій, створений Paul Rouget у 2012 року, який містить в собі HTML-каркас, CSS-стилі, JS-скрипти. Особливістю даного варіанту є його мінімальність у використанні лише одного файлу, який включає в собе всю презентацію. Медіа-контент завантажується ззовні, з Інтернет-джерела, вказаного в лістингу.

3. Shower - за словами автора, Вадима Макеєва, «двигун для створення презентацій», створений у 2010 році. У цього «двигуна» є наступні особливості:

- Додавання стилів в окремий слайд здійснюється через його id.
- Для спрощення розподілу тексту на дві колонки реалізований клас «double».
- Освітлення програмного коду здійснюється в тегу <code> за допомогою тегу <mark> і двох класів: «comment» і «important».

Також в цьому напрямку можна відзначити наступні JS-фреймворки, які використовують HTML5 і CSS3:

4. Reveal.js - JS-фреймворк, який у 2011 року створив Hakim El Hattab. Особливостями цього JS-фреймворка є:

- Підтримка взаємодії з Grunt (інструментом для збирання проектів).
- Підтримка CSS-зупинки презентації за допомогою «згасання» екрану.
- Підтримка ефектів переміщення між слайдами (Fade, Slide, Convex, Concave, Zoom, Cube, Page, None)
- Підтримка Parallax background.
- Підтримка конвертування презентації в формат .pdf.
- Підтримка «лінивого завантаження» – завантаження зовнішніх файлів за їх необхідністю.
- Можливість встановлення часового інтервалу для кожного слайду.
- Реалізований плагін для підтримки використання Markdowna.

5. Impress.js - JS-фреймворк, який у 2011 року створив Bartek Szopka. Особливість цього JS-фреймворка полягає в можливості маніпулювання координатами слайду в «3D-просторі» презентації, кутом нахилу слайда, його масштабом.

6.deck.js - JS-фреймворк, який у 2011 році створив Caleb Troughton. Особливостями цього JS-фреймворка є:

- Автоматичне масштабування презентації, маніпулювання цим процесом.
- Кожен слайд – об’єкт jQuery.

Отже, розглянувши вищевказані варіанти, можна підсумувати, що синтез HTML5, CSS3 и JavaScript може бути вдалою основою реалізації презентацій. Цей синтез може проявлятися, як у вигляді фреймворків (CSS- або JS-), так і у вигляді одного HTML-файлу.

Таким чином, представленні варіанти своїми можливостями здатні надати можливості для створення незвичайних презентацій без залежності від традиційно використовуваного для цих цілей ПЗ.

УДК 004.94

Імітаційне моделювання руху школярів на графі “школа-житло”

Маліченко Є.П., учениця 11-го класу, учениця Малої академії наук учнівської молоді
Науковий керівник – Дрєєв О.М., к.т.н., викладач
Кіровоградський обласний навчально-виховний комплекс
(гімназія – інтернат – школа мистецтв), м. Кіровоград

В роботі розглянуто процес укрупнення навчальних закладів по типу школи-інтернату. За законодавчими нормами проведено аналіз документів та отримано залежності витрат держави на одного учня за навчальний рік. Зроблено висновок про можливість не лише значного заощадження державних коштів при укрупнені навчальних закладів але й підвищення якості навчання. Але при створені моделі “школа-житловий район” для розрахунків середнього часу проведеного учнями в дорозі та витрат держави та сім’ями на траспортні послуги, виникла ситуація неоднозначного розподілу учнів між шкільними закладами. Щоб отримати придатні до використання результати було вирішено використати імітаційне моделювання.

Передбачається використання програми для різних моделей та ситуацій, тому було вирішено зберігати моделі в xml-форматі, де присутній перелік шкіл з параметрами та районів проживання. Також в моделі присутні зв’язки-маршрути, які містять ідентифікатори району та школи з вартістю проїзду. Так утворюється граф, який зберігається в програмі у вигляді трьох списків відповідних класів “школа”, “район”, “автобус”.

З причини, що граф можна показати різними розміщеннями вершин, в програмі передбачено перегляд з розміщенням за спіралями, півколами, колами та лінійні розміщення. На рисунку 1 показано розміщення по колам для моделі Кіровоградської області:

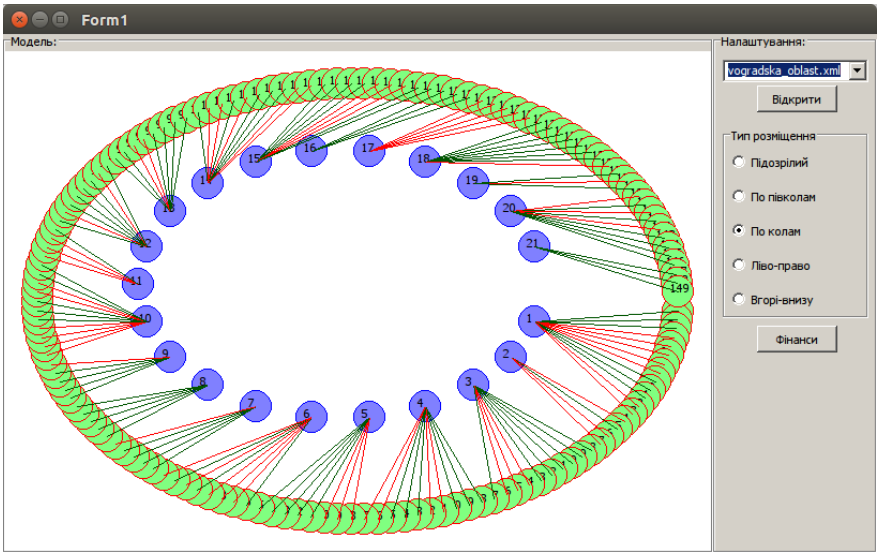


Рисунок 1 — Граф моделі “школа-житло” в розташуванні вершин колами

Для довільної моделі, в загальному випадку, ситуація можливості пересування школярів з одного району проживання до різних шкіл є природною. Тому, виникає неоднозначність в розрахунках часу, який в середньому учень проводить в дорозі, та грошей витрачених учнями за оплату проїзду. Проблему вирішено розв’язувати за допомогою імітаційного моделювання. Для цього створено процес, коли з множини транспортів обирається випадковий екземпляр. Обраний транспорт пов’язаний фіксованим маршрутом, і для нього відбувається перевезення максимально можливої кількості учнів до школи. Для одиничного акту перевезення враховуються параметри:

1) кількість учнів ще недоставлених до школі в районі маршруту;

2) кількість вільних місць в школі;

3) кількість місць в транспорті.

З причини, що маршрут обирається випадково, можлива ситуація, коли в деяких школах залишилися місця, але можливостей перевезення учнів немає. Наприклад, школа є заповненої з сусіднього району, а додаткових маршрутів не заплановано. Тому моделювання проводиться до перевезення 90% всіх учнів, що практично в усіх випадках дозволило отримати результати моделювання. В цьому випадку отримані результати коригуються з коефіцієнтом 10/9.

Імітаційне моделювання є по суті низкою випадкових подій. Тому результати одного моделювання може відрізнятися від іншого. З цієї причини моделювання проводиться 10 разів у циклі, а результати усереднюються. Звіт такого моделювання для тестової моделі показано на рисунку 2:

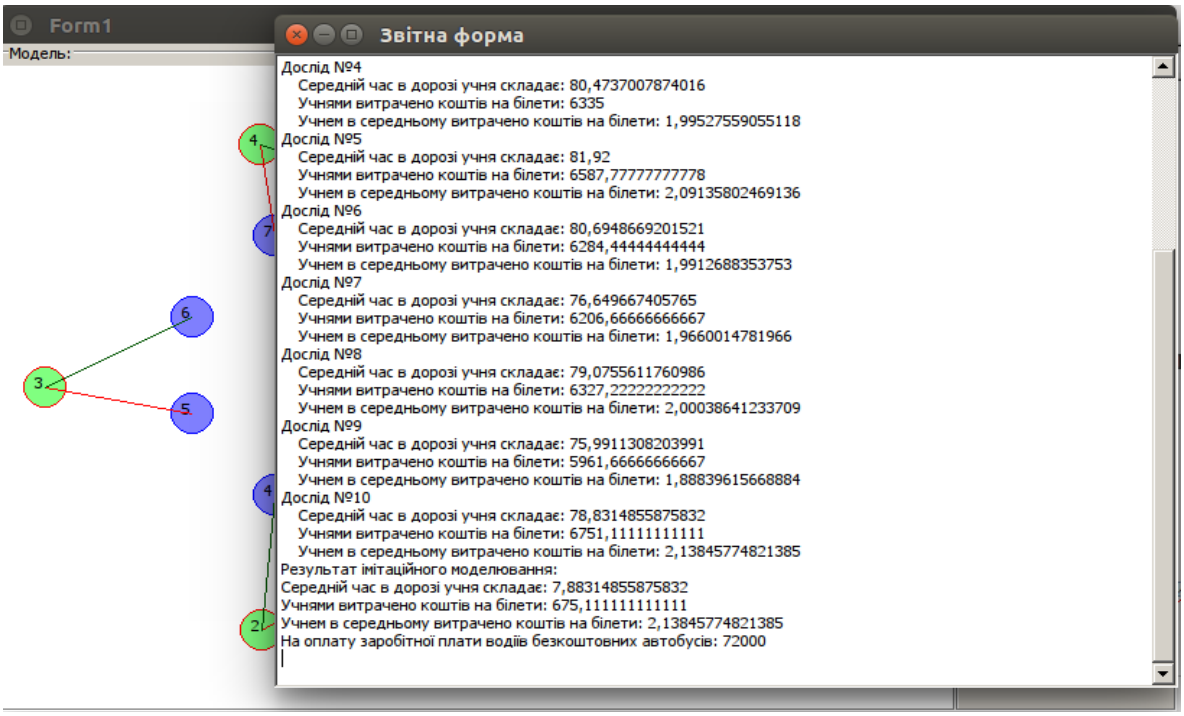


Рисунок 2 — Результати моделювання пересування учнів до школи

Висновки. В результаті розв’язування задачі оцінювання витрат часу учнів та грошових витрат на пересування до школи, було реалізовано імітаційну модель на випадкових подіях. Отримана модель дозволила отримати на тестових моделях розумні результати, що підтверджує її правильність та застосовність.

Список літератури

1. Алексеев Е.Р., Чеснокова О.В., Кучер Т.В. Самоучитель по программированию на Free Pascal и Lazarus. - Донецк.: ДонНТУ, Технопарк ДонНТУ УНИТЕХ, 2011. - 503 с.

2. Кетков, Ю. Л. Свободное программное обеспечение. FREE PASCAL для студентов и школьников / Ю. Л. Кетков, А. Ю. Кетков. — СПб.: БХВ-Петербург, 2011. — 384 с.

3. Мансуров К.Т. Основы программирования в среде Lazarus, 2010. – 772 с.

4. Бакнелл Джулиан М. Фундаментальные алгоритмы и структуры данных в Delphi: Пер. с англ./Джудиан М. Бакнелл. - СПб: ООО “ДиаСофтЮП”, 2003. - 560 с.

УДК 004.522

Актуальність та основні проблеми реалізації технологій автоматичного розпізнавання мови для вбудованих систем

Мартинюк І.А., аспірант, igoraspirant@ro.ru
Науковий керівник – Лахно В.А., д.т.н., доцент
Європейський університет, м.Київ

На сучасному етапі розвитку інформаційних технологій постає проблема зручного та ефективного способу взаємодії людини з інформаційними системами. Оскільки усне мовлення є природнім способом спілкування для людини, технології автоматичного розпізнавання мови, в свою чергу, дозволять їй найбільш ефективно взаємодіяти з такими системами.

Використання систем автоматичного розпізнавання мови відкриває широкий спектр застосувань: від додатків для автоматичного набору тексту і транскрибації аудіозаписів до управління бортовими пристроями автомобілів та автоматизації процесів систем масового обслуговування (наприклад, збору показників лічильників для комунальних служб).

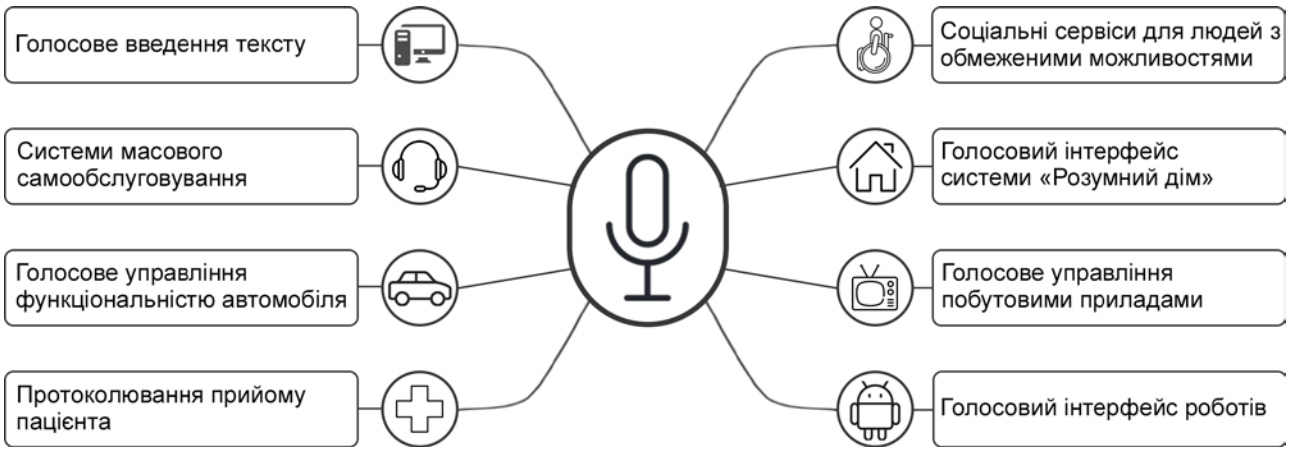


Рисунок 1. Основні сфери застосувань систем автоматичного розпізнавання мови

Актуальність застосування систем розпізнавання мови для вбудованих систем. Типово, системи автоматичного розпізнавання мови реалізовуються у вигляді програмних додатків для персональних комп'ютерів чи серверів (хмарні обчислення), оскільки потребують значних обчислювальних потужностей та ресурсів для розпізнавання мови в реальному часі. Проте, така реалізація накладає ряд обмежень, зокрема щодо портативності та автономності пристроїв, які використовують дану технологію.

Реалізація систем розпізнавання мови для вбудованих систем у вигляді автономних портативних модулів (плат розширення) дозволить обійти дані обмеження та ефективно використовувати ці системи у таких областях, як автотранспорт, авіація, соціальна сфера, робототехніка тощо.

Прикладом застосування таких систем може слугувати голосове управління функціоналом автомобіля (для якого помилка розпізнавання не призведе до аварійної ситуації), тим самим розвантажуючи водія, щоб він міг сконцентрувати свою увагу на дорозі. Інший приклад – реалізація мовного інтерфейсу в інвалідних кріслах для людей з обмеженими можливостями.

Структурна схема процесу автоматичного розпізнавання мови. Процес розпізнавання умовно можна поділити на два етапи: розпізнавання частин мови та визначення найбільш вірогідного варіанту слова із словнику. В загальному, даний процес можна описати послідовністю основних кроків (див. рис. 2).

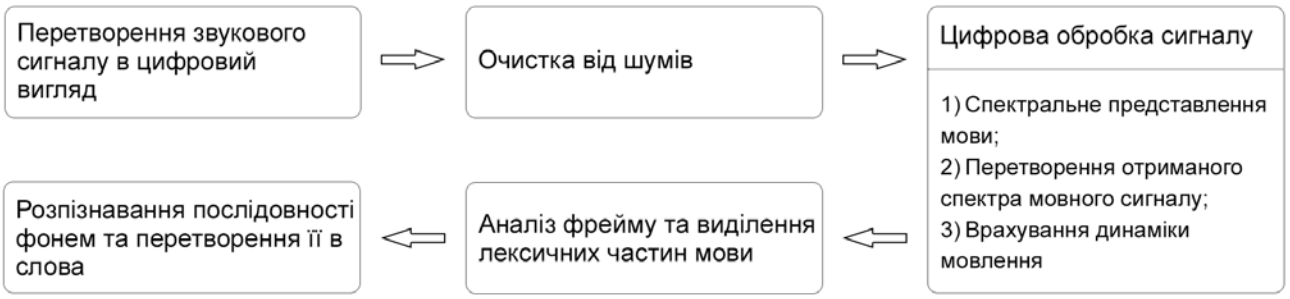


Рисунок 2. Структура процесу автоматичного розпізнавання мови

Складність реалізації систем розпізнавання мови. Взаємодія з інформаційними системами за допомогою голосу полягає у принципових відмінностях людського мовлення від традиційних способів введення інформації. Програми, як правило, очікують точних вхідних даних, але людська вимова не досить чітка, кожен людський голос значною мірою відрізняється, швидкість та інтонація може змінюватись, крім того існує складність з визначенням відповідності фонем, які в деяких випадках звучать однаково.

Для того щоб реалізувати всі необхідні етапи з відповідними їм алгоритмами в режимі реального часу та якісно розпізнати мову, необхідно мати в наявності достатньо обчислювальних ресурсів.

Іншою проблемою є необхідність зберігання та швидкого доступу до бази слів для реалізації другого етапу розпізнавання.

Для вирішення проблеми недостатньої кількості обчислювальних ресурсів можна покластись на останні розробки в області мікропроцесорної техніки.

На сьогодні існують мікропроцесорні ядра Cortex-M4 та Cortex-M7, розроблені ARM Holdings, які мають у своєму складі арифметичний співпроцесор, який дозволяє ефективно виконувати операції з дійсними числами, та модуль цифрової обробки сигналів, за допомогою якого можна виконувати цифрову фільтрацію та перетворення Фур'є, яке необхідне для спектрального представлення звукового сигналу.

Продуктивність таких ядер досягає 2.14 DMIPS/MHz, а існуючі мікроконтролери на їх базі мають ефективність в понад 400 DMIPS. Крім того, вони мають у своєму складі модуль прямого доступу до пам'яті та аналого-цифровий перетворювач.

Для оптимізації зберігання та пошуку слів із бази можна спроектувати окремий модуль, апаратну СУБД, який буде працювати з базою даних розміщеною на карті пам'яті та обмінюватиметься інформацією з основним модулем через послідовний інтерфейс, наприклад UART. Реалізація СУБД у вигляді окремого модуля дозволить зекономити обчислювальні ресурси та зосередитись на основних задачах розпізнавання.

Висновки. Обґрунтовано актуальність розробки систем автоматичного розпізнавання мови для вбудованих систем. Висвітлено основні проблеми та складності реалізації таких систем, а також запропоновано шляхи їх вирішення.

Список літератури

1. Cortex-M Series [Електронний ресурс]. – Режим доступу: http://www.arm.com/products/processors/cortex-m/
2. STM32F7 Series [Електронний ресурс]. – Режим доступу: http://www.st.com/web/en/catalog/mmc/FM141/SC1169/SS1858/
3. *Винцюк Т.К.* Анализ, распознавание и интерпретация речевых сигналов. Киев: Наук. думка, 1987. – 264 с.
4. *Фролов А.В., Фролов Г.В.* Синтез и распознавание речи. Современные решения. – М.: Связь, 2003. – 216 с.

УДК 621.396.67

Метод моделирования сетевого пакетного трафика

Мачалин И.А., профессор, д.т.н., проф., Одарченко Р.С., доцент, к.т.н.,
Тараненко А.Г., доцент, к.т.н., доц., Габрусенко Е.И., доцент, к.т.н., доц.,
e-mail: igor.machalin@ukr.net
Национальный авиационный университет, г. Киев

Моделирование пакетного трафика является достаточно актуальной задачей, поскольку позволяет анализировать и синтезировать телекоммуникационные сети с заданными параметрами обеспечения качества. Особенности трафика в сетях с пакетной коммутацией, а именно, статистические плотности распределения с «тяжелыми хвостами» и бесконечными дисперсиями [1] не всегда можно адекватно описать аналитическими моделями. Поэтому необходимо найти алгоритм, позволяющий упростить задачу моделирования. Основным свойством пакетного трафика является его самоподобность (фрактальность). Как показано в работе [2] этими же свойствами обладают так называемые клеточные автоматы, предложенные Нейманом. В докладе авторы предлагают метод, позволяющий относительно несложно получить математическую модель пакетного трафика с помощью клеточных автоматов, которые также обладают свойствами фрактальности. Учитывая возможности самообучения клеточных автоматов, можно предположить, что их использование в моделировании пакетного трафика приведет к значительному упрощения проектирования сетей.

Клеточные автоматы являются математической идеализацией физических систем, в которых пространство и время являются дискретными, а физические величины принимают на конечном множестве дискретные значения. Клеточный автомат состоит из регулярной равномерной решетки, обычно конечной степени, с дискретными переменными. Состояние клеточного автомата полностью определяется значением переменных на каждом участке, которые обновляются одновременно, основываясь на значении переменных в их районе на предыдущем шаге по времени. Показатели производительности обычно получают с помощью компьютерного моделирования эволюции клеточного автомата с течением времени.

Модель базируется на том предположении, что пакетный трафик также, в определенном смысле, состоит из «частиц» - документов (сообщений). Для формирования модели мультимедийного трафика с произвольными параметрами предлагается метод моделирования на основе многослойного клеточного автомата и рекурсивных перестановок. Сущность метода заключается в использовании двух независимых многослойных клеточных автоматов с промежуточными связями между слоями и матрицами рекурсивных перестановок, сохраняющие окрестности для формирования двух векторов случайных значений, интерпретирующийся как интервал времени и значение трафика на данном интервале.

Метод позволяет формировать модели самоподобного мультимедийного трафика с необходимыми статическими характеристиками за счет управления состояниями слоев клеточного автомата и порядком их выбора при формировании вектора интервала времени. Компьютерное моделирование показало достаточно хорошую адекватность данного метода при сходимости к статистическим данным до 10%. Дальнейшим развитием данных исследований является анализ и исследование других видов само подобных клеточных автоматов для моделирования телетрафика.

Список литературы

1. Шелухин О. И. Причины самоподобия телетрафика и методы оценки показателя Херста // Электротехнические и информационные комплексы и системы. – Вып.1, Т.3. – 2007.-С. 5–13.

5. Нейман Дж. Теория самовоспроизводящихся автоматов. – М.: Мир, 1971. – 382с.

УДК 621.391 (043.2)

Моделювання роботи мережі SDN на базі віртуальних комутаторів за технологією Overlay

Одарченко Р.С., к.т.н., доцент, odarchenko.r.s@mail.ru
Національний авіаційний університет, м. Київ

Сьогодні комп'ютерні мережі є необхідною частиною будь-якого підприємства, навчального закладу, державної організації тощо. Сучасні КМ не позбавлені недоліків, таких як: складність управління мережею, висока вартість мережевого обладнання, недостатньо ефективне використання каналу зв'язку через передавання великої кількості інформації для керування мережею замість корисного трафіку тощо. Концепція SDN (Software-Defined Networking – програмно-конфігурована мережа) – відносно нова технологія у сфері телекомунікацій, покликана виправити ці недоліки. Програмно-конфігурована мережа (SDN – Software-Defined Networking) сьогодні є однією з найперспективніших технологій у галузі комп'ютерних мереж. Модель SDN має ряд переваг над традиційними мережами, серед яких розробники виділяють наступні: підвищення ефективності мережевого обладнання на 25-30%; зниження на 30% витрат на експлуатацію мереж; надання користувачам можливості програмно створювати нові сервіси і оперативно завантажувати їх в мережеве обладнання.

Концепція SDN передбачає розділення площин трафіку і управління [1]. Спрощена архітектура зображена на рис.1. В SDN-мережах весь інтелект апаратного забезпечення (площина управління) переноситься до єдиного центру – контролера. Таким чином, SDN-комутатори – прості пристрої, єдиною функцією яких є комутація і передача даних (функція площини трафіку). Робота контролера може бути частково чи повністю автоматизована завдяки програмним додаткам, що самостійно керують мережевими ресурсами. Контролер приймає всі рішення, базуючись на повному баченні мережі і застосовує їх одночасно до усіх пристроїв мережі. Наприклад, при надходженні великого потоку трафіку, правил маршрутизації якого комутатор не знає, контролер приймає рішення один раз для усіх пристроїв; в традиційній мережі кожен пристрій має здійснювати маршрутизацію окремо. Сигнальна інформація надходить до нього по окремим каналам, ізольованим (часто фізично) від каналів передачі даних. Все це покращує ефективність роботи мережі і збільшує швидкість обробки даних, особливо для великих об'ємів трафіку.

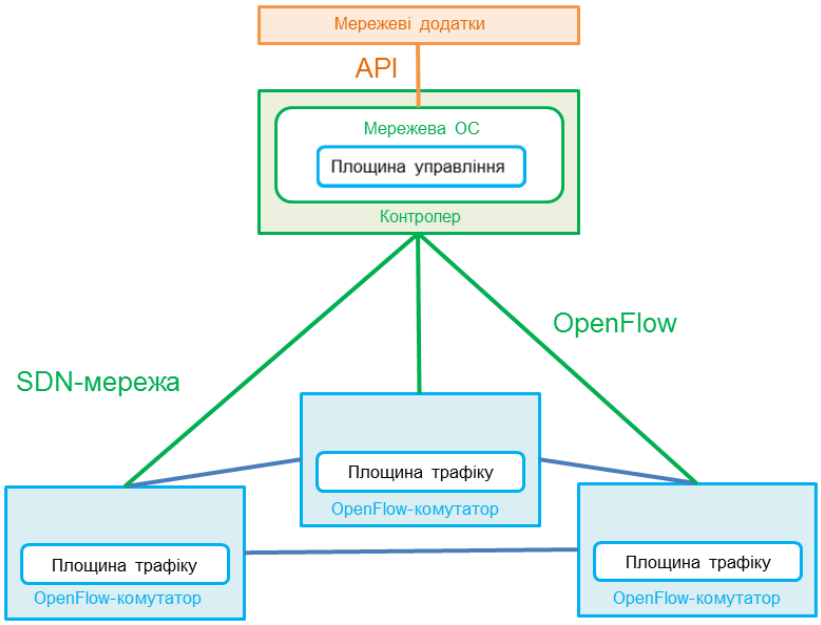


Рис.1. – Спрощена архітектура SDN-мережі

Реалізація концепції SDN на практиці дозволить операторам ISP (Internet Service Provider) отримати незалежний від виробників обладнання контроль над всією мережею з єдиного місця, що значно спростить її експлуатацію. Що не менш важливо, конфігурування мережі сильно спроститься, і адміністраторам не доведеться вводити сотні рядків коду окремо для різних комутаторів або маршрутизаторів. Характеристики мережі можна буде оперативно змінювати в режимі реального часу, відповідно, терміни впровадження нових додатків і сервісів значно скоротяться.

Для реалізації SDN-мереж використовують два основних методи [2]:

- **Реалізація SDN на базі спеціальних комутаторів (протокол Openflow).**

При такій побудові мережі в якості мережевого обладнання використовуються комутатори, які для взаємодії з контролером використовують протокол Openflow. При цьому інше обладнання, таке як IP-комутатори та маршрутизатори, не використовується в «чистій» SDN-мережі.

- **Реалізація SDN на базі віртуальних комутаторів за технологією Overlay.** Така SDN-мережа може бути побудована поверх звичайної мережі , при цьому до фізичного комутатора чи маршрутизатора приєднується запущений на гіпервізорі віртуальний комутатор (наприклад Open vSwitch), що підтримує протокол Openflow (рис. 2). Весь трафік, що надходить на фізичний пристрій, пересилається на програмний комутатор, де відбувається його маршрутизація. Після цього трафік відправляється потрібному адресату з фізичного комутатора.

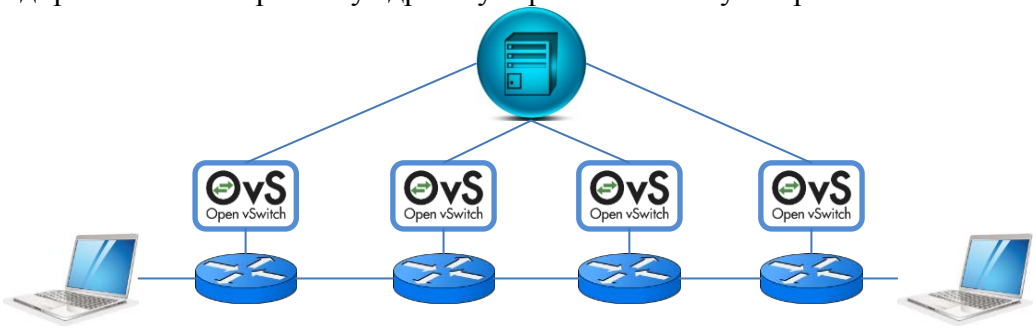


Рис. 2. - Спрощена топологія SDN/Overlay-мережі

Висновки. В роботі було проведено аналіз архітектури та концепції мереж SDN. Проведено аналіз можливостей, які надає даний підхід до реалізації комп'ютерних мереж. Програмно-конфігуровані мережі дозволяють користуватись широким розширеним функціоналом для управління комп'ютерними мережами. Також в роботі було проведено дослідження архітектури Overlay-мереж SDN. Проаналізовано переваги та недоліки двох методів реалізації SDN. Overlay мережі можуть бути побудовані поверх будь-якої сучасної IP-мережі без заміни обладнання, крім того їх можливо будувати на оптичних мережах. Але в порівнянні з апаратним підходом такі мережі мають більшу затримку. Проведено моделювання роботи Overlay мережі з використанням програмних комутаторів Open vSwitch з допомогою ПЗ Mininet та MiniEdit. Аналіз отриманих результатів доводить, що використання SDN мереж ефективніше за використання IP мереж при великих об'ємах трафіку та при великій кількості мережевого обладнання.

Список літератури

1. Черняк Л.В. SDN – от замысла до рынка // Открытые системы. – 2012. – № 09.
2. Семенов Ю.А. Сетевая технология OpenFlow (SDN). – ИТЭФ-МФТИ, 2014.

УДК 004.9

Програмне забезпечення для розв'язування функціональних рівнянь

Олійник Ю.І., учень 11-го класу, учень Малої академії наук учнівської молоді
Науковий керівник – Дрєєв О.М., к.т.н., викладач
Кіровоградський обласний навчально-виховний комплекс
(гімназія – інтернат – школа мистецтв), м. Кіровоград

В роботі поставлено задачу розв'язання функціональних рівнянь виду

$$h\left(\frac{m}{n^k}\right) = a_0 h\left(\frac{m}{n^{k-1}} - 0\right) + a_1 h\left(\frac{m}{n^{k-1}} - 1\right) + \ldots + a_{n-1} h\left(\frac{m}{n^{k-1}} - (n-1)\right),$$

де m, n, k є цілими, а $h(t)=0$ при $t\le 0$ та $h(t)=1$ при $t\ge 1$, коефіцієнти a — довільні дійсні константи.

Огляд літератури та аналіз рівняння показав відсутність методу знаходження розв'язку рівняння у вигляді формули. Тому було вирішено побудувати чисельний метод.

Використати табличне задання функції з покроковим поповненням цієї таблиці дозволив доведений факт, що при відомих значеннях $h(m/n^{k-1})$, можна отримати проміжні значення функції $h(m/n^k)$. Тому при початковому значенні $k=1$, для пошуку проміжних значень m/n можна використати лише початкові значення $h(0)=0$ та $h(1)=1$.

З метою перевірки застосовності методу було використано електрону таблицю, де за допомогою прямих формул розв'язувалося рівняння при $n=2$ та $n=3$. Отримані таблиці підтвердили застосовність методу, але мала кількість точок не дає змогу оцінити вигляд функції. Задача створення програми для розрахунку достатньої кількості значень функції та побудови її графіку стає актуальною.

Вигляд головного вікна створеної програми показано на наступному рисунку:

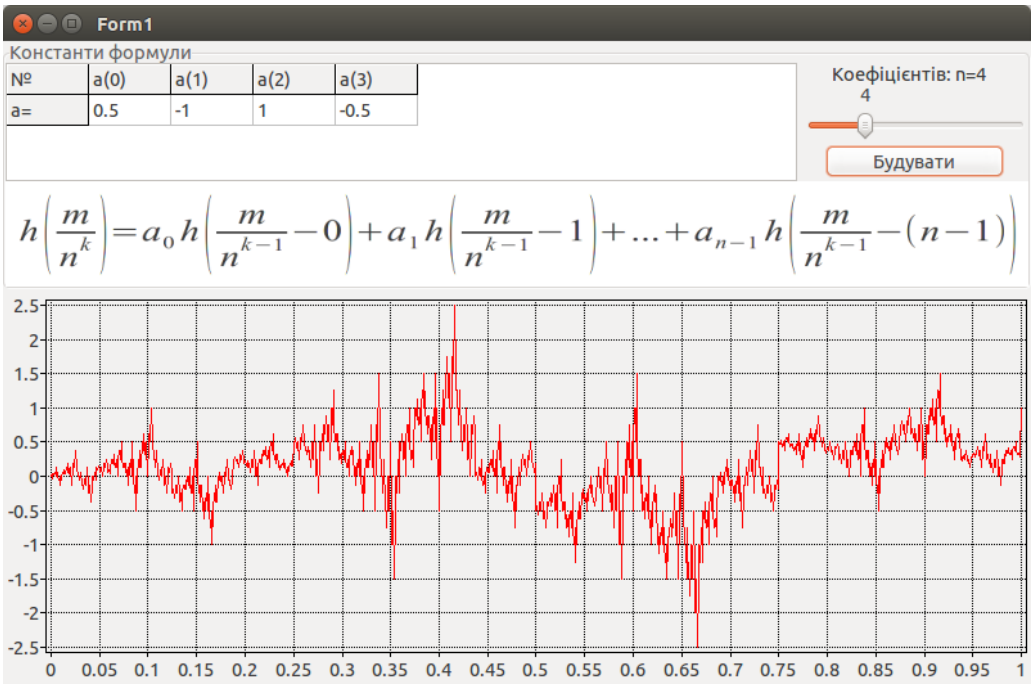


Рисунок 1 — Приклад розв'язку рівняння з чотирма коефіцієнтами

Отриманий графік має явно сильно коливний вигляд, що нагадує сигнал з накладанням сильного шуму. На наступному рисунку показано розв'язок рівняння з трьома коефіцієнтами $a_0=a_2=0{,}5$; $a_1=-0{,}5$.

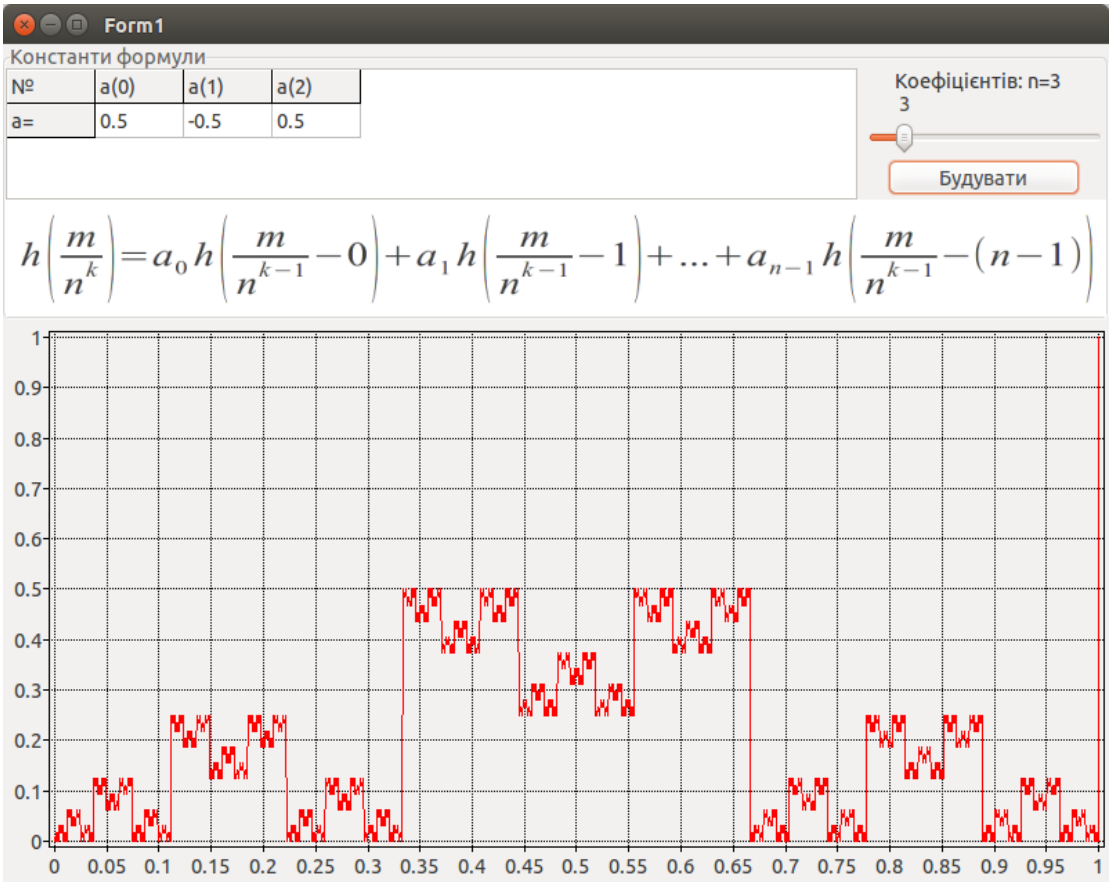


Рисунок 2 — Отриманий графік-розв'язок нагадує фрактал

Останній графік з рис. 2 зовнішнім виглядом нагадує фрактальну криву, що дає обґрунтування вважати, що формула (1) задає криві з самоподібними властивостями.

Висновки. В результаті отримано програмне забезпечення, яке з заданою точністю визначає табличні значення функції h(t). Шукана функція має фрактальну природу.

Список літератури

1. Алексеев Е.Р., Чеснокова О.В., Кучер Т.В. Самоучитель по программированию на Free Pascal и Lazarus. - Донецк.: ДонНТУ, Технопарк ДонНТУ УНИТЕХ, 2011. - 503 с.

2. Кетков, Ю. Л. Свободное программное обеспечение. FREE PASCAL для студентов и школьников / Ю. Л. Кетков, А. Ю. Кетков. — СПб.: БХВ-Петербург, 2011. — 384 с.

3. Мансуров К.Т. Основы программирования в среде Lazarus, 2010. – 772 с.

4. Ахо, Альфред, В., Хопкрофт, Джон, Ульман, Джеффри Структуры данных и алгоритмы. : Пер. с англ. : М. : Издательский дом "Вильяме", 2003. — 384 с.

5. Бакнелл Джулиан М. Фундаментальные алгоритмы и структуры данных в Delphi: Пер. с англ./Джудиан М. Бакнелл. - СПб: ООО "ДиаСофтЮП", 2003. - 560 с.

6. Бенуа Б. Мандельброт. Фрактальная геометрия природы = The Fractal Geometry of Nature. — М.: Институт компьютерных исследований, 2002. — С. 656.

УДК 004.6

Розробка програмного забезпечення для аналізу соціальних мереж Social Network Analyzer

Охотний С.М., студент 2 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент, elismeleshko@gmail.com
Кіровоградський національний технічний університет, м. Кіровоград

На даному етапі розвитку суспільства значний вплив на поведінку людей здійснюють соціальні Інтернет-мережі (Facebook, VKontakte, Twitter, та багато інших).

На сьогоднішній день соціальні мережі стали інструментом впливу та прихованого контролю над соціумом. Масштаби такого контролю можуть варіюватися від просування різних товарів до організації масових суспільних протестів (Туніс, Гонконг, Великобританія, Україна).

Аналіз соціальних мереж дає можливість виявляти ймовірності та шляхи поширення вірусної інформації у суспільстві, знаходити учасників мережі, які намагаються маніпулювати свідомістю інших або потенційно можуть це робити.

Розроблене програмне забезпечення (ПЗ) Social Network Analyzer (SNA) дає можливість виконувати аналіз соціальної мережі за певним типом алгоритму. В базовій комплектації для аналізу доступна одна соціальна мережа ВКонтакті, та один алгоритм для виявлення найвпливовіших учасників мережі.

В архітектуру даного ПЗ була закладена технологія динамічних розширень – плагінів (plugins), які дають можливість розширювати функціонал програми за допомогою динамічних бібліотек, при цьому перекомпіляція основного додатку не потрібна. SNA самостійно сканує відповідні директорії з плагінами і додає їх. Таким чином в майбутньому є можливість створювати нові розширення для соціальних мереж та алгоритмів їх аналізу.

Для виконання аналізу необхідно спершу завантажити інформацію про користувачів та зв’язки між ними з соціальної мережі (процес завантаження відображено на рисунку 1).

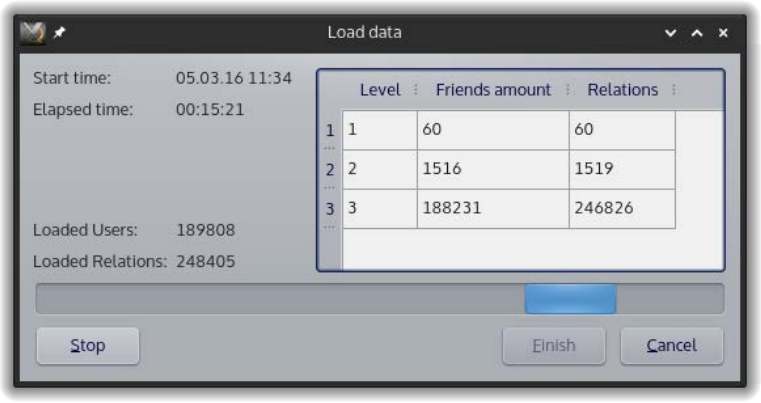


Рисунок 1 – Процес завантаження даних у Social Network Analyzer

Під зв’язками розуміються усі друзі кожного користувача. SNA надає можливість зібрати такі дані. Завантажена інформація організовується в окремій базі даних і представляється в програмі у вигляді графа (користувачі мережі – вершини, зв’язки – ребра).

Збір інформації виконується на основі рекурсивного обходу всіх друзів відносно опорного користувача з певною глибиною (враховуються друзі друзів до вказаної глибини), яка задається в початкових налаштуваннях при створенні нового графу (бази даних).

Для роботи додатку необхідно, щоб на комп’ютері був встановлений MySQL-сервер. На ньому створюються необхідні бази даних для зберігання завантажених даних.

Алгоритм пошуку найвпливовівших друзів опорного користувача передбачає калькулювання значень впливовості для кожного з них, які базуються на відношенні кількості зв’язків кожного користувача в межах заданої рекурсії до всіх зв’язків, що містить граф. Таким

чином для кожного користувача знаходиться значення впливовості, яке представляється дійсним числом в межах від 0 до 1.

Додаток надає можлвість встановлення параметрів відбору користувачів соціальної мережі за певними параметрами (типи і кількість таких параметрів залежать від реалізації конкретного плагіна алгоритму аналізу графа). Кожен параметр може бути увімкненим або вимкненим. Приклад налаштування параметрів показано на рисунку 2.

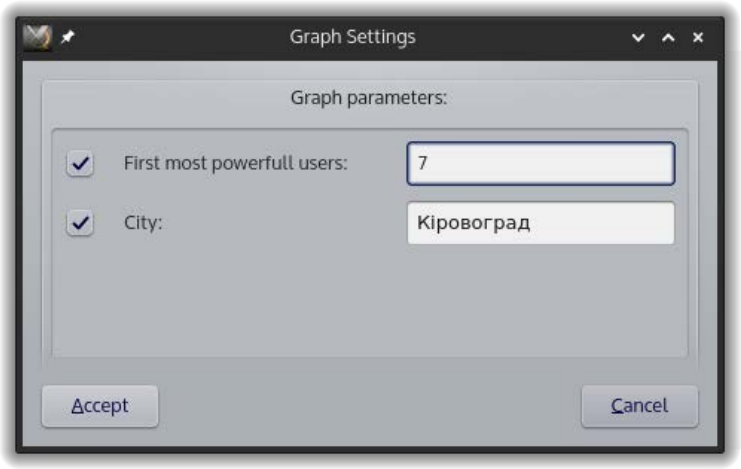


Рисунок 2 – Налаштування параметрів вибірки користувачів для аналізу

У базовій комплектації плагін алгоритму аналізу впливовості надає два параметри:

- число перших найбільш впливоих друзів опорного користувача;
- місто, в межах якого виконуватиметься аналіз.

На рисунку 3 показано приклад побудованого графу (другого рівня рекурсії), що містить сім перших найвпливовіших друзів та друзів друзів опорного користувача мережі Вконтакті, у яких найвищий показник впливовості серед 544 представників міста Кіровограда, що увійшли до вибірки.

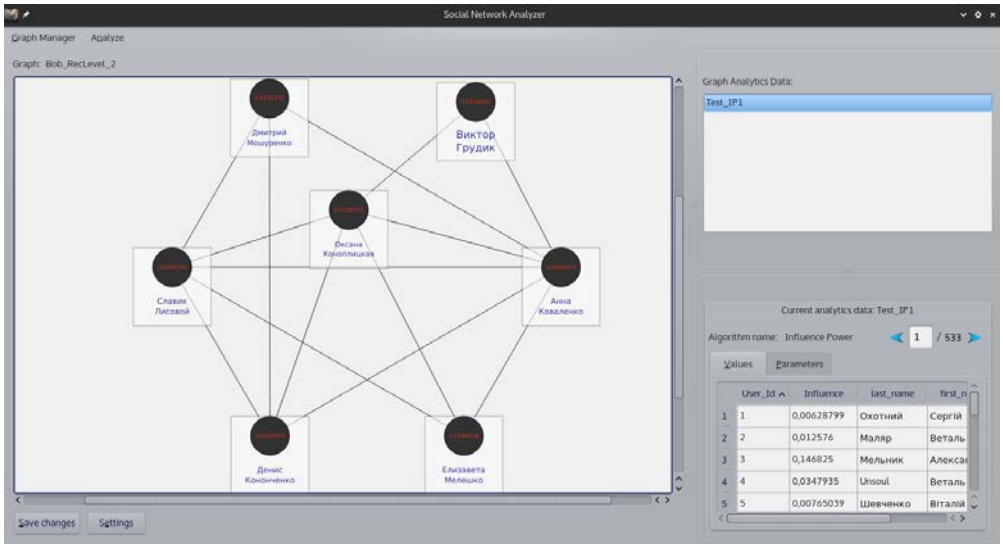


Рисунок 3 – Відображення графу зв’язків між сімома найвпливовішими друзями та друзями друзів з міста Кіровограду опорного користувача мережі Вконтакті

УДК 004.021 + 004.58 + 004.4'6

Система оцінки знань програмного інженера

Паливода Є.В., студент, jekainfinity@gmail.com,
Куницька С.Ю., к.т.н., доцент kunitskaya33@gmail.com
Черкаський державний технологічний університет, м. Черкаси

Стрімкий розвиток технологій привів до активного збільшення кількості програмних продуктів та засобів, які використовуються для керування даними технологіями та створення нових. В свою чергу поява великої кількості програмного забезпечення призводить до того що люди все більше цікавляться, як ці програми функціонують і прагнуть самі освоїти, як створити дані продукти. Люди, які починають цікавитись даним питанням, а саме питанням програмування, дуже часто стикаються з проблемою нерозуміння того, чи вони рухаються в правильному напрямку і чи правильно вони це роблять. Це являться проблемою, тому що людина починає зупинятись в своєму розвитку і може взагалі опустити руки, втративши інтерес до програмування.

Запропонований програмний продукт вирішує цю проблему, він допоможе людям, які хочуть розвиватись побачити, чого вони досягли і чи в правильному напрямку вони рухаються, а також дозволить оцінити свої навички тим людям, які вже освоїли програмування в певній мірі.

Програмний продукт являє собою веб-систему, основною задачею якої є оцінка знань програмного інженера. Оцінка знань полягає в тому, що користувач, який і являється програмним інженером, проходить набір тестів. Кожен тест являє собою задачі різної степені тяжкості, на вирішення яких відводиться певний час і ставляться певні умови. Пройшовши тести користувач отримує оцінку, яка відповідає його навичкам. Головними аспектами по яких буде оцінюватись програмний код являється відповідність специфікаціям вибраної мови програмування та забезпечення проходження набору тестів.

Для розробки веб-системи використовується мова Java. Java – це мова для розробки корпоративного програмного забезпечення, для розробки мережевих та веб сервісів. Дана мова була обрана для реалізації системи так як вона забезпечує надійність, гнучкість та масштабованість. Також мова Java є кросплатформенною, тобто програми написані на ній можуть виконуватись на машинах з різною архітектурою та операціними системами, що полегшує подальше супроводження та переносимість.

Як середовище розробки було вибрано IDE Intlijj IDEA Ultimate 15, яка являє собою одну з найпопулярніших середовищ розробки в даний час, вона підтримує роботу з багатьма фреймворками та дозволяє включити в проект багато розширень та плагінів. Також дана IDE дає змогу легко синхронізуватись з системою контролю версій, якою в даному проекті виступає GIT. GIT одна з найефективніших систем контроля версій, яка надає гнучкі методи розробки проекту.

Для роботи з веб середовищем було вирішено використати фреймворк Spring Framework, який реалізує патерн MVC(Model-View-Controller). Шаблон MVC поділяє систему на три частини, так щоб кожна із частин не впливали на розробку інших частин. Даний фреймворк також реалізовує IoC (inversion of control), що являє собою принцип побудови програми, при якому її частини отримують потік керування з загальної області. В проекті використовується принцип IoC при ін'єкції компонентів в інші класи.

Доступ в систему мають лише зареєстровані користувачі або адміністратори, тому потрібно реалізувати розмежування прав та привілегій. Для того, щоб реалізувати захист системи від несанкціонованого доступу та забезпечети розмежування прав між користувачами використовуватиметься технологія Spring Security, яка являє собою JavaEE Framework.

Система використовує багато залежностей на інші ресурси та бібліотеки, які знаходяться в глобальному репозиторії(сховищі), дані ресурси будуть з'єднуватись з проектом за допомогою засобу автоматизації роботи з програмними проектами Maven. Дана система також здійснює установку плагінів, які відповідають за розвернення даного проекту на веб сервері.

Для того щоб система працювала як веб-додаток необхідно її запустити на HTTP-сервері, в

ролі даного сервера було використано вільний контейнер сервлетів Jetty, який написаний на мові Java. Jetty являється одним з провідних контейнерів сервлетів на даний момент. Його перевагами є те, що він економно використовує память і використовує NIO, що дозволяє Jetty обслуговувати велику кількість користувачів в одиницю часу.

Система зосереджена на роботу з даними користувача та іншими даними, як наприклад, тести, їх потрібно зберігати в базі даних. Для роботи з базами даних було вибрано систему керування реляційними базами даних MySql. MySql володіє високою швидкістю виконання команд, простотою використання та наявністю простої та ефективної безпеки, що в свою чергу робить її ідеальним варіантом для використання при проектуванні веб-системи.

Так як Java це мова яка підтримує обєктно орієнтовану парадигму програмування, то є доцільним виражати і працювати в програмі не з окремими даними з бази даних, а з даними, які представленні у вигляді обєктів. Щоб реалізувати дану можливість система використовує технологію ORM Hibernate, яка звязує реляційну базу даних з концепціями об'єктно орієнтованих мов програмування. Перевагою Hibernate над звичайними запитами являється спрощення типових задач при роботі з базою даних та представлення таблиць у вигляді обєктів, для того щоб реалізувати цю можливість необхідно створити класи, які будуть містити ті ж самі поля, що й в таблиці, для того щоб отримані дані були розміщенні в екземплярах даного класу.

Висновки. Було показано проблему, що виникає при навчанні людей, яка полягає в тому, що люди часто не розуміють, як їм переступити певну межу в програмній інженерії і чи знання, які вони отримали з різних ресурсів є правильними. Було запропонованно рішення даної проблеми у вигляді системи, яка являє собою систему оцінки знань програмного інженера, шляхом проходження певного набору тестових задач.

Список літератури

1. Hibernate ORM Documentation (5.0) [Електронний ресурс] – режим доступу http://hibernate.org/orm/documentation/5.0/.

2. Apache Maven Documentation [Електронний ресурс] – режим доступу http://maven.apache.org/guides/.

3. Java Tutorial Guide [Електронний ресурс] – режим доступу http://www.mkyong.com/tutorials/java-io-tutorials/.

4. Git tutorial and training [Електронний ресурс] – режим доступу https://www.atlassian.com/git/tutorials/.

5. Spring Guide [Електронний ресурс] – режим доступу https://spring.io/.

6. Spring in Action, Fourth Edition // Крейг Уолс- 2014 – с. 624.

7. Структуры данных и алгоритмы JAVA // Роберт Лафоре – Питер 2013 – с.704.

8. Beginning Java Programming: The Object-Oriented Approach //Bart Baesens, Aimee Backiel, Seppe vanden Broucke – 2015 – с. 672.

УДК 004.6 +004.7+004.652

Розробка мобільного додатку для управління спільними покупками на основі операційної системи Apple «iOS»

Прозапас В.О., студент, danteakuma7@gmail.com,
Куницька С.Ю., к.т.н., доцент, kunitskaya33@gmail.com
Черкаський державний технологічний університет, м. Черкаси

Розвиток мобільної техніки – це не тільки розвиток елементної бази та зменшення основних компонентів для створення смартфону, це й стрімкий розвиток мобільних операційних систем, програмних компонентів, додатків та ін.

Мобільний додаток для управління спільними покупками грає велику роль у повсякденному житті кожної людини. Кожного дня кожна людина має справу з грошима, а особливо з розрахуванням боргів. Дуже часто виникають ситуації коли знайомі, приятелі або просто друзі повинні швидко розрахувати певну суму на кількох чоловік. Таке часто трапляється при спільному відпочинку в певному закладі. При чому, дуже часто це зробити тяжко лише за допомогою одного калькулятора: занадто багато потрібно тримати в голові або виписувати в окреме місце. Мобільний додаток для управління спільними покупками легко може вирішити дану проблему. В даній системі кожен користувач може зареєструватись під своїм логіном. Для здійснення розрахунку по спільним покупкам кожен користувач може знаходитись в певній групі, для якої і розраховується потрібна сума. Для розробки мобільного додатку було обрано пристрої на основі операційної системи «iOS», через те, що відсоток пристроїв на основі платформи iOS від усіх мобільних пристроїв в світі становить 25.6%. Разом з цим, статистика показує, що кількість пристроїв Apple зростає з кожним днем, так як виходять все більш нові версії операційної системи та самих пристроїв.

На ряду із стрімким розвитком мобільних технологій та необхідності у швидкому та зручному розрахуванні спільних покупок для певних груп людей, було прийнято рішення про створення простого, швидкого та зручного мобільного додатку на пристрої, що працюють під платформою iOS.

Загальна структура мобільних додатків на платформі iOS. Розглянемо загальну схему створення мобільних додатків на платформі iOS та методи взаємодії між її компонентами. Схема, що зображена на рисунку 1 носить назву «MVC» - Model – View – Controller. Схема MVC є основною для всіх, хто розробляє мобільні додатки під платформу iOS. Вона була впроваджена і затверджена самими розробниками Apple. Тому, оригінальні додатки від Apple створюються саме по такій схемі.

Даний мобільний додаток буде працювати під платформи iOS і мовою програмування для його створення є Objective-C, так як саме Objective-C є зручною в користуванні та швидкою в взаємодії між компонентами мовою програмування. Так як лише одної мови програмування недостатньо, для створення додатку буде використано програмний системний каркас (фреймворк) під назвою Cocoa Touch. Цей фреймворк буде відповідати за роботу сенсорних клавіш, взаємодію між компонентами екранів. Мобільний додаток буде містити в собі також мобільну базу даних для швидкого користування та перегляду можливої історії. Для підключення бази даних буде використано SQLite.

За передачу даних між екранами, взаємодію контролерами один з одним буде використано ще один програмний каркас під назвою Core Data. Обов’язково додаток буде мати можливість завантажувати дані з мережі, тому для такого буде використано бібліотеки SCNetworkReachability, AFNetworking, JSONModel. Передача даних між сервером та пристроями буде здійснюватися за допомогою JSON-рядка тексту. Такий спосіб забезпечить максимальну швидкість та надійність в передачі.

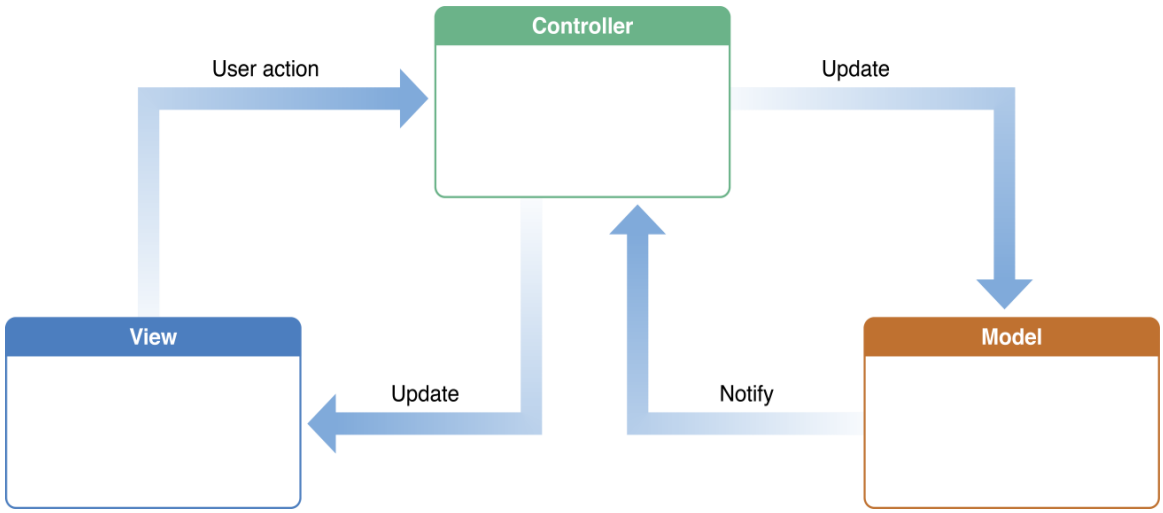


Рисунок 1 – Структурна схема взаємодії між компонентами платформи iOS

Отже, для створення додатку під мобільну платформу iOS буде використано базові фреймворки Cocoa Touch та Core Data, основну бібліотеку для підключення бази даних – SQLite, білбіотеки для роботи з мережею - SCNetworkReachability, AFNetworking. Дані від сервера будуть отримуватись та відправлятись на сервер у вигляді одного рядку тексту у форматі JSON. Вся організація і принципи роботи будуть відповідно структури створення мобільних додатків під iOS від Apple – MVC.

Висновки. Даний мобільний додаток реалізує простий доступ до управління спільними покупками певних груп людей. Завдяки швидкому та економічному обміну інформацією з сервером, архітектурою створення мобільних додатків MVC та мові програмування Objective-C додаток буде працювати швидко, без затримок та без використання великих об'ємів пам'яті для передачі інформації між сервером та додатком. Завдяки всім вищезгаданим системним фреймворкам та основам створення мобільних додатків від Apple, даний мобільний додаток буде мінімалістичним, зручним у використанні та простим у дизайні. Так як компанія Apple слідкує за розповсюдженням продукції на їх пристрої, то єдиним можливим варіантом поширення даного мобільного додатку буде тільки завантаження його до онлайн інтернет-магазину від компанії «Apple» - AppStore. Завдяки онлайн магазину AppStore користувачі самі зможуть знаходити даний мобільний додаток, використовуючи тільки основні теги, що характеризують сам додаток та його роботу.

Список літератури

1. Apple Developer [Електронний ресурс]. – Режим доступу: https://developer.apple.com.
2. MVC Patter [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Model-View-Controller.
3. Cocoa Touch [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Cocoa_Touch.
4. SQLite Tutorial [Електронний ресурс]. – Режим доступу: http://www.tutorialspoint.com/ios/ios_sqlite_database.htm.
5. Stephen G. Kochan, Programming in Objective-C, 6th Edition // Addison-Wesley Professional, p. 551.

УДК 004.75

Технологія побудови систем доставки контенту на основі розподілених хеш-таблиць

Сергєєв А.В., аспірант, a.serhieiev@gmail.com
Науковий керівник – Порєв Г.В., д.т.н., доцент
Київський національний університет імені Тараса Шевченка, м. Київ

Розповсюдженість географічно розосереджених мереж призвела до появи проблем, пов'язаних із затримкою доступу до потрібної користувачеві інформації, у випадку значної географічної віддаленості між сервером та клієнтом.

Можливим рішенням таких проблем є використання систем доставки контенту (CDN – Content Distribution Network) – структури, що оптимізує розподіл контенту до кінцевих користувачів мережі. Принцип роботи CDN полягає у взаємодії георграфічно розподілених локальних серверів, які зберігають копії файлів основного серверу і намагаються підтримувати їхню актуальну версію. Таким чином клієнту мережі не обов'язково робити запити до центрального серверу, а потрібно знайти географічно найближчу його копію. Це допомагає не тільки зменшити затримку при пошуку необхідної інформації, але й зменшити навантаження на основний сервер, що значно підвищує надійність всієї системи.

Нажаль, розгортання такої системи потребує значних фінансових ресурсів, тому доступна лише для комерційних структур. Компаніям з обмеженним фінансуванням необхідно використовувати ресурси всіх елементів мережі для розподілу інформації, щоб не підтримувати коштовну інфраструктуру серверів-реплікацій, які мають бути достатньо потужними для забезпечення відмовостійкості мережі навіть при значних навантаженнях.

Базою для глобальної системи доставки контенту доцільно використовувати однорангові (p2p) мережі, в яких кожен елемент є одночасно і клієнтом і сервером. У порівнянні з клієнт-серверною архітектурою в таких мережах відсутні проблеми із масштабованістю та надійністю.

Для створення однорангових мереж необхідні ефективні алгоритми пошуку інформації. Для їх реалізації прийнято використовувати розподілені хеш-тиаблиці (DHT – Distributed Hash Table) – оверлейну структуру, що працює за принципом асоціативного масиву, тобто інформація знаходиться за допомогою певного ключа, який у свою чергу є результатом деякої хеш-функції від назви файлу у якому інформація зберігається. Найвідомішим сервісом, побудованним на основі DHT є BitTorrent.

Наразі існує багато різних, як теоретичних так и практичних реалізацій DHT [1]. Тим не менш питання реалізації CDN на основі DHT залишається відкритим. На даний час існує лише декілька спроб реалізацій таких систем. Серед них слід виділити Coral CDN [2] – єдину систему такого типу, що працювала у реальних умовах, але через певні недоліки перестала обслуговувати клієнтів у 2012 році.

Висновки.

Реалізація системи доставки контенту на основі розподіленої хеш-таблиці може допомогти у створенні глобальних географічно розосереджених мереж, користування якими буде комфортним для кінцевого користувача та не буде потребувати значних фінансових витрат з боку розповсюджувача.

Список літератури

1. H. Balakrishnan, M. Kaashoek, D. Karger, and I. Stoica, 2003. "Looking up data in p2p systems." Comm. ACM 46, 2(Feb.)

2. M. J. Freedman, E. Freudenthal, and D. Mazieres. Democratizing content ` publication with Coral. In NSDI, Mar. 2004.Проблемы передачи данных в сетях мобильной связи

УДК 004.652+004.43

Розробка серверного додатку для роботи з програмами для управління груповими покупками на платформах Android та IOS

Смалько Ю.С., студент, smalkoy@gmail.com,
Бабенко В.Г., к.т.н., доцент, zolot_verba@rambler.ru,
Куницька С. Ю., к.т.н., доцент, kunitskaya33@gmail.com
Черкаський державний технологічний університет, м. Черкаси

Масштабне поширення смартфонів з високими показниками продуктивності та безкоштовною операційною системою Android дозволяє розробникам програмного забезпечення створювати засоби для спрощення повсякденних задач людини. Однією з таких задач є обрахунок фінансових взаємодій між людьми на побутовому рівні. Для вирішення цієї задачі запропоновано додаток для управління груповими покупками для смартфонів з операційною системою Android.

Для повноцінної роботи додатку необхідний сервер обробки даних. Для стартового запуску та тестування додатку було використано ресурс під назвою Parse, який надає можливість обробки даних без програмування та розгортання власного серверного додатку, звернення до сервера відбувається шляхом використання Parse API (application programming interface), що дозволяє використання сервера для роботи з простими структурами даних. В подальшій розробці додатку було виявлено складність та громіздкість запитів (request) та відповідей (response) сервера, що призводить до уповільнення роботи з додатком, а у випадку з повільним з'єднанням з мережею Internet, до майже неможливого використання додатку.

Було запропоновано створити власний серверний додаток та розмістити його на хмарній платформі. Було обрано платформу Heroku, яка є хмарною PaaS-платформою (Platform as a service), яка надає доступ до інформаційно технологічних платформ для розміщення та розгортання додатків. Для розробки серверного додатку обрано трирівневу модель архітектури додатку, яка передбачає наявність в ньому трьох компонентів: клієнта, сервера додатків (до якого підключено додаток клієнта) та сервера баз даних (з яким працює сервер додатків).

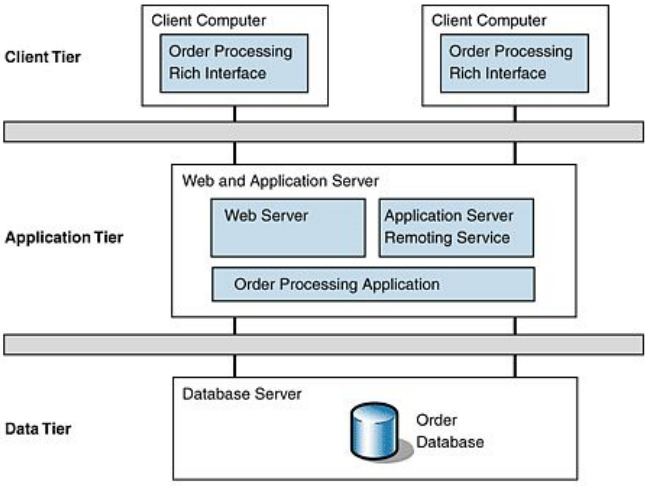


Рисунок 1 - Трирівнева модель архітектури додатку

Клієнт – інтерфейсний (зазвичай графічний) компонент комплексу, який надається кінцевому користувачу. Даний рівень не має прямого зв'язку з базами даних, не навантажується бізнес логікою і не зберігає стан додатку. На даний шар виноситься лише базова валідація внесеної користувачем інформації. Сервер додатків виконує основну частину бізнес логіки за виключенням лише експортовані на клієнт термінали, а також елементи логіки завантажені в базу даних (збережені процедури та трігери). Даний шар є ланкою, яка зв'язує клієнт з сервером баз даних. Сервер баз даних забезпечує збереження даних та мають зв'язок лише з засобами систем

управління базами даних, які забезпечують підключення до цього компоненту тільки з рівня серверу додатків.

Мовою програмування для реалізації даного проекту обрано мову з о'бєктно-орієнтованою парадигмою Java. Так як дана вона крос платформною, зручною для реалізації ентерпрайз-додатків та має масу бібліотек для роботи з різними ресурсами. Для реалізації третього шару, а саме серверу баз даних вирішено використати базу даних реляційного типу на базі технології MySQL, так як реляційна база найкращим чином відповідає вимогам даного додатку. Для спрощення роботи з СУБД вирішено застосувати систему ORM (object relation mapping), яка зв'язує бази даних з концепціями об'єктно-орієнтованих мов програмування, створюючи «віртуальну об'єктну базу даних». Використовуватися буде бібліотека Hibernate, яка представляє собою вільне програмне забезпечення з відкритим кодом (open source). Дана бібліотека представляє зручний фреймворк для відображення об'єктно-орієнтованої моделі даних в традиційні реляційні бази даних. Для доступу до бази даних розробляється ряд об'єктів, в сукупності складають відображення сутностей (entities), кожен з яких відповідає таблиці реляційної бази даних, для цього створюються об'єкти з вказанням відповідних полів, описаних анотаціями, забезпеченими бібліотекою Hibernate.

Для отримання чи занесення даних кожному об'єкту-сутності ставиться у відповідність DAO (Data Access Object), в якому реалізується методи для маніпуляції даних, але тільки базових маніпуляцій, таких як вибірка даних з базі за визначеними параметрами, запис даних та інших операцій спрямованих на взаємодію з об'єктами бази даних. Наступним шаром об'єктів є шар сервісів (services), які забезпечують коректне відображення інформації для запобігання збоїв в роботі програми. Загальне компонування додатку вирішено здійснювати за допомогою програмного каркасу Spring Framework, який представляє собою програмний каркас з відкритим кодом та контейнер з підтримкою інверсії управління (inversion of control), впровадження залежностей (dependency injection), управління танзакціями, Модель-Вигляд-Контролер (Model-View-Controler), тестування та ряду інших можливостей для платформи Java.

Model-View-Controler – архітектурний шаблон, який використовується під час проектування та розробки програмного забезпечення, який поділяє систему на три частини: модель даних, вигляд даних та керування. Застосовується для відокремлення даних від інтерфейсу користувача так, щоб зміни інтерфейсу користувача мінімально впливали на роботу з даними, а зміни в моделі могли здійснюватися без змін інтерфейсу користувача.

Для взаємодії з Android та IOS додатками буде представлено API-бібліотеку з документацією, яка описує порядок складання запитів на стороні додатку до серверу та вміст відповідей, якими буде реагувати сервер на дані запити. У відповідях будуть міститися JSON (JavaScript Object Notation) об'єктами

Висновки. Даний серверний додаток реалізує простий і надійний доступ до інформації розміщеної в базі даних на сервері, з її подальшою перевіркою, обробкою та представленням у вигляді узгодженому з додатками для платформ Android та IOS, у відповідь на чітко сформульовані запити. Об'єднаний програмний комплекс збереже час для людей, які часто здійснюють групові покупки.

Список літератури

1. Walls C. Spring in action: 4-th edition // Manning Publications Co. USA. – p.626.
2. Bauer C., King G., Gregoru G. Java Persistence with Hibertnate, Second edition // Manning. USA. – p.608.
3. Three tier architecture [Електронний ресурс]. – Режим доступу: http://www.cardisoft.gr/frontend/article.php?aid=87&cid=96.
4. MVC [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Model-View-Controller.

УДК 004.92

Программирование анимированной компьютерной графики на платформе JAVAFX

Смирнова Н.В., канд. техн. наук, доцент, snvkntu@rambler.ru,
Смирнов В.В., канд. техн. наук, доцент, swckntu@rambler.ru
Кировоградский национальный технический университет

Платформа JavaFX реализует несколько методов анимации, из них наиболее известные - анимация по ключевым кадрам, которая реализована классами `Timeline` и анимация со встроенной временной шкалой, которая реализована классом `Transition`.

Анимация по ключевым кадрам позволяет создать видимое изменение значения любого JavaFX-свойства за определенный промежуток времени с помощью класса `Timeline`.

Для объекта класса `Timeline` можно установить частоту кадров и набор ключевых кадров анимации. Коллекция ключевых кадров `Timeline`-анимации пополняется методом `getKeyFrames().addAll()`. Запуск объекта анимации осуществляется методом `play()`, а остановка - методом `stop()`.

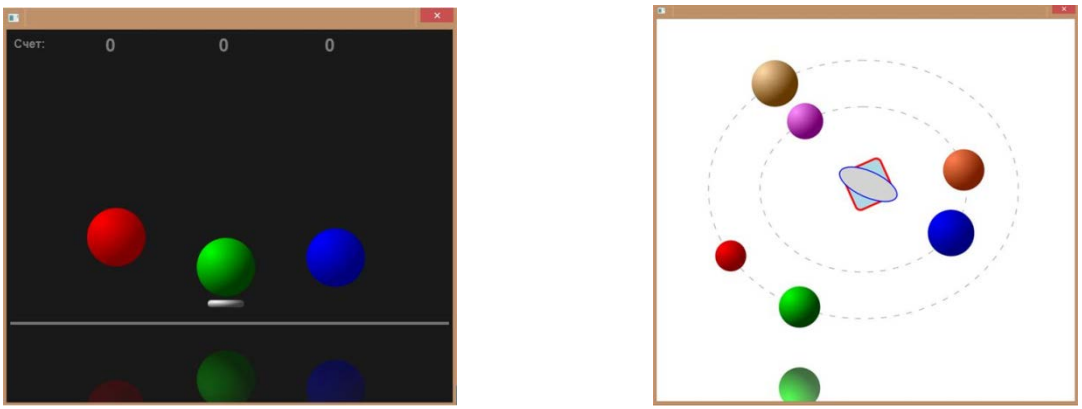
Ключевой кадр `Timeline`-анимации реализован классом `javafx.animation.KeyFrame`, в котором определяются изменения значений свойств объекта анимации за определенный период времени.

Объект класса `KeyFrame` можно создать с помощью набора конструкторов, позволяющих установить время воспроизведения ключевого кадра, имя ключевого кадра, обработчик окончания ключевого кадра и набор изменений значений `JavaFX`- свойств

`Transition`-анимация со встроенной временной шкалой использует объект `Interpolator` в качестве значения свойства `interpolator` класса `Transition`.

Таким образом, анимацию объектов на основе изменения их свойств можно создать двумя методами. Первый - это создание одного ключевого кадра `KeyFrame` и с последующим добавлением в него нескольких объектов класса `KeyValue`. Второй - это создание отдельных ключевых кадров `KeyFrame` для каждого из объектов `KeyValue` и добавление их в `Timeline`-анимацию (рис.1 а)). Анимация пространственного положения узла графа сцены создается с помощью классов `PathTransition` и `TranslateTransition`.

Класс `PathTransition` позволяет создавать перемещение графического объекта вдоль произвольно заданного пути (рис.1 б)).



а) б)

Рис. 1 – Анимация с использованием классов `Timeline` и `PathTransition`

Класс `TranslateTransition` позволяет создавать перемещение графического объекта из одной 3D-точки в другую 3D-точку (рис.2).

Рис. 2 – Анимация с использованием класса `TranslateTransition`

В JavaFX существует возможность объединения нескольких анимаций объектов в их последовательность с помощью класса `SequentialTransition`. В этом случае завершение одной анимации является началом следующей. Параллельное выполнение анимаций реализовано в классе `ParallelTransition`. Таким образом, становится возможным создание мультипликации. Пауза в последовательности анимаций реализована классом `PauseTransition`. Важный класс `AnimationTimer` позволяет создавать таймер, вызываемый в каждом кадре анимации. Для управления таймером класс `AnimationTimer` испльзует методы `start()` и `stop()` (рис.3).

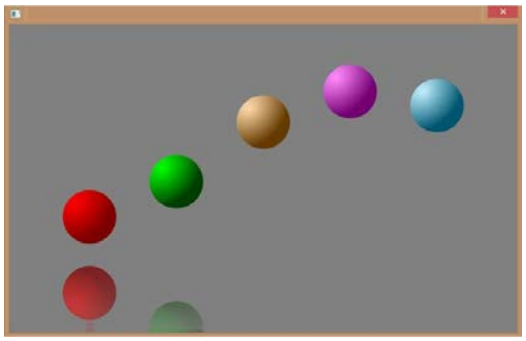


Рис. 3 – Анимация с использованием классов `ParallelTransition` и `AnimationTimer`

Трансформации узлов графа сцены, состоящие из аффинных преобразований: вращений, перемещений, масштабирования и сдвига реализует пакет `javafx.scene.transform`.

В отличие от анимации, трансформации графических объектов не имеют плавного видимого перехода от начальной точки к конечной точке в течение определенного промежутка времени. Классы, реализующие аффинные преобразования, позволяют преобразовать n-мерный объект, при этом сохраняя параллельность линий и плоскостей, а также пропорции параллельных объектов с учетом искажений перспективы.

Таким образом, платформа Java/JavaFX предоставляет большие возможности для создания и анимации сложных графических объектов, в частности для построения моделей процессов, для создания многопользовательских компьютерных игр, интерфейса пользователя и т.д.

Список литературы

1. Тимур Машнин JavaFx 2.0: Разработка RIA-приложений / Тимур Машнин. – Спб.: БХВ-Петербург, 2012. - 320 с.
2. http://www.oracle.com/
3. http://docs.oracle.com/apps/searchttparch.jsp?category=java&product=&q=JavaFx
4. Johan Vos Pro JavaFX 8 / Johan Vos, Weiqi Gao, 2014. – APRESS. – 604 p.
5. Carl Dea JavaFx 8: Introduction by Example / Carl Dea, Mark Heckler. - APRESS, 2014. - 420 p.

УДК 519.582

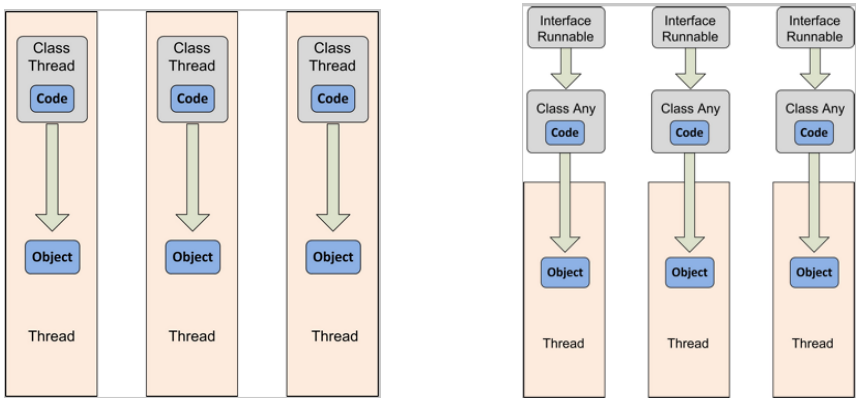
Особенности многопоточного программирования на платформе JAVAFX

Смирнов В.В., канд. техн. наук, доцент, swckntu@rambler.ru,
Смирнова Н.В., канд. техн. наук, доцент, snvkntu@rambler.ru
Кировоградский национальный технический университет

В настоящее время существуют различные реализации параллелизма выполнения программ, в общем случае, разделяемые на параллелизм процессов и на параллелизм потоков в рамках одного процесса. Традиционно, поток в Java создается и управляется методами класса `Thread`. После создания объекта этого класса одним из его конструкторов новый поток запускается методом `start()`. Поэтому объект класса `Thread` сам является потоком (рис. 1 а)).

Более совершенным вариантом многопоточности является создание потока путем расширения интерфейса `Runnable`. Интерфейс в Java является аналогом заголовочного файла языка программирования C и C++. Методы в интерфейсе, как и в заголовочном файле объявлены, но не реализованы.

Интерфейс `Runnable` содержит всего один метод `run()`. Поэтому в классе, который расширяет интерфейс `Runnable` необходимо реализовать объявленный в нем метод `run()`(рис.1.б)).



а) б)

Рис. 1 – Расширение класса `Thread` и расширение интерфейса `Runnable`

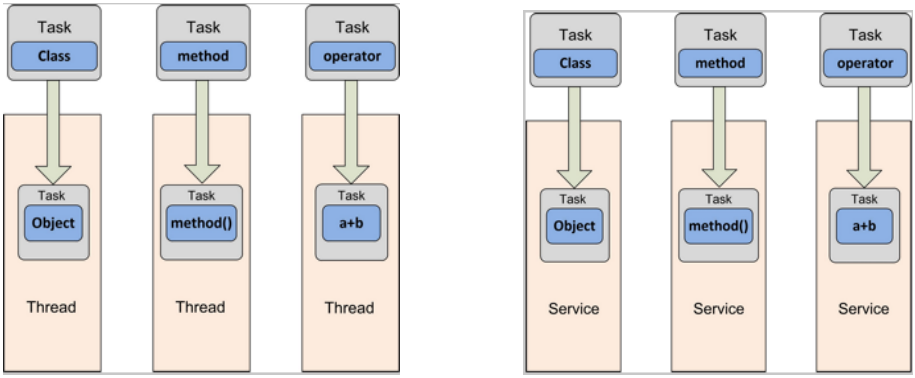
С появлением многоядерных процессоров возникла потребность в более развитых средствах создания потоков и управления ими. Поэтому состав JDK включены пакеты `java.util.concurrent`.

Пакеты содержат интерфейсы и классы, облегчающие работу с потоками. Основу пакета составляет интерфейс `Callable`, описывающий один метод `call()`.

В отличие от метода `run()` метод `call()` возвращает результат. Результатом может быть произвольный объект. Поэтому более современным способом создания и запуска потоков является использование пакета `java.util.concurrent`.

В частности, класс `Task` позволяет запускать в потоке объекты классов, отдельные методы и отдельные операторы. Поэтому использование класса `Task` повышает гибкость программы (рис. 2 а)).

Использование `пакета java.util.concurrent` также предполагает запуск задач в потоках с помощью класса `Service` (рис. 2 б)).



а) б)

Рис. 2 – Использование класса `Task` и класса `Service`

Создание нового потока - это операция, потребляющая много ресурсов, поскольку она включает в себя взаимодействие с операционной системой. Если в программе создается большое количество кратковременных потоков, то имеет смысл использовать пул потоков.

Пул потоков может иметь несколько простаивающих свободных потоков, готовых к запуску. То есть, в разное время разные задачи используют свободные потоки для своего выполнения. Если задача выполнена, то поток, в котором выполнялась задача, не уничтожается, как обычно, а становится доступным для выполнения другой задачи.

Другая причина для использования пула потоков – это необходимость ограничить количество параллельно выполняющихся потоков. Создание огромного числа потоков может отрицательно сказаться на производительности и даже привести к полному отказу виртуальной машины. Пулы потоков используют класс `Executors`.

Для реализации высокоскоростных вычислений для больших массивов данных в Java реализован фреймворк `Fork-Join` - метод, применяемый в коммуникационных и компьютерных системах и служащий для увеличения производительности выполнения большого количества рабочих задач.

Метод заключается в том, что каждая задача разбивается на множество синхронизированных задач, которые обрабатываются параллельно на разных процессорах и/или серверах. Большая задача рекурсивно разбивается на более мелкие подзадачи, где количество подзадач определяется заданным порогом. Данный этап называется `Fork`.

Результат выполнения параллельных подзадач объединяется до тех пор, пока не будет решена главная задача. Данный этап называется `Join`.

Производительность вычислений существенно возрастает с увеличением количества процессоров, задействованных в процессе вычислений. Количество параллельных потоков, выполняемых процессорами может быть задано или ограничено в процессе создания программы вычислений.

Таким образом, платформа Java/JavaFX позволяет программисту выбрать необходимые средства реализации многопоточности, оптимальные для решения конкретной задачи.

Список литературы

1. http://www.oracle.com/
2. http://docs.oracle.com/apps/searchttparch.jsp?category=java&product=&q=JavaFx
3. Johan Vos Pro JavaFX 8 / Johan Vos, Weiqi Gao, 2014. – APRESS. – 604 p.
4. Carl Dea JavaFx 8: Introduction by Example / Carl Dea, Mark Heckler. - APRESS, 2014. - 420 p.

УДК: 004.056.55

Направления использования технологии Blockchain

Стеценко П.И., студент VI курса, steps.ps@rambler.ru,
Нияченко С.А., студент VI курса, nceregao@mail.ru
Научный руководитель – д.т.н., проф. Халимов Г.З.
Харьковский национальный университет радиоэлектроники

Интерес финансовых институтов к технологии Blockchain крайне велик, хотя бы потому, что использование Blockchain банками может существенно снизить годовую стоимость инфраструктуры. В свою очередь, некоторые крупные банки, например, как UBS, создали лабораторию для исследования Blockchain, а Goldman Sachs, NASDAQ и некоторые другие крупные финансовые учреждения инвестируют в Bitcoin стартапы.

Технология Blockchain позволяет совершать сделки в условиях отсутствия доверия, обеспечивая достаточный уровень защищенности и без привлечения третьей доверенной стороны. Так как нет посредника при совершении сделки, то весь процесс становится проще, быстрее и дешевле. Эта концепция может быть применена ко всему цифровому миру, делая любой вид обмена/транзакций безопасными и доступными. В данной работе проведен анализ направлений использования технологии Blockchain и компаний, которые, соответственно, начинают развиваться на основе этой технологии.

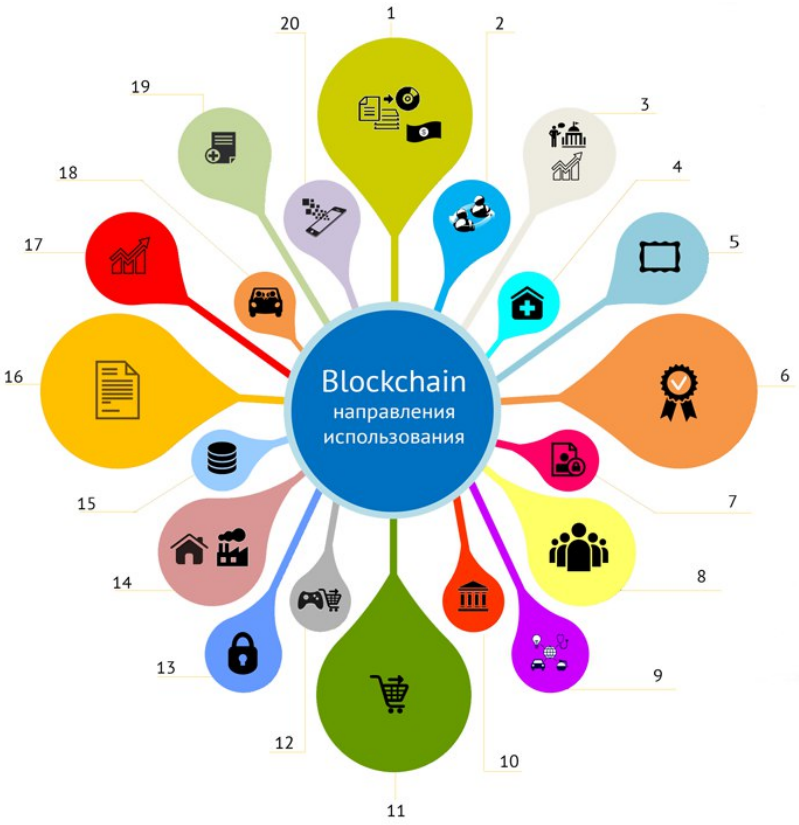


Рисунок 1 – Направления использования технологии Blockchain

На рисунке 1 приведено визуальное представление направлений, которые развиваются на основе технологии Blockchain:

1) доказательство права собственности и сегмент рынка купли-продажи цифровых активов (компания MyPowers);

2) предоставление возможности гарантированной подлинности рецензии:

- посредством надежных подтверждений для сотрудника-рецензента (компании TRST.im, Asimov);

- позволяет привлекать пользователей, распространять отзывы и получать обратную связь (компания The World Table);

3) децентрализованная платформа прогнозирования фондовых рынков, политики и т.п. (компания Augur);

4) децентрализованное управление записями (карточками) пациентов (компания BitHealth (Healthcare IT));

5) доказательство собственности цифрового контента – статей, фотографий и изображений (компании: Blockai, Bitproof, ascribe, Artplus, Stampery);

6) оцифровка активов: существенно снижает вероятность подделок. Компании в сфере бытовой техники и автомобилестроения: The Real McCoy, ChainLink. Компания Degree of Trust занимается верификацией ученых степеней – это технологическая платформа, которая связывает профили выпускников в социальной сети с их учеными степенями и использует защищенные коммуникации с поставщиками исходных данных с помощью технологии Blockchain;

7) обеспечение цифровой идентификации, которая защищает конфиденциальность потребителя:

- в Интернете – компания Onename;

- идентификация клиента – компания Trustatom;

8) системы электронного голосования (компания Follow My Vote, BitCongress);

9) децентрализованный Интернет и вычислительные ресурсы для отдельных пользователей и бизнеса (компания ePlug);

10) децентрализованное учреждение обществ (компаний), передача прав долевого участия / собственности и полномочий управления (компания Otonomos);

11) предоставление услуг по созданию и выполнению смарт-контрактов – протоколов, позволяющих автоматизировать финансовые/коммерческие контракты (компания UbiMS);

12) услуги депозитария:

- игровая индустрия (компании PlayCoin, Bitnplay);

- игровая индустрия и обслуживание платежей (компания New System Technologies);

13) электронная коммерция (компания Funds.org);

14) децентрализованный Интернет вещей (Internet of things):

- домашняя автоматизация (компания Chimera-inc);

- автоматизация производства (компания Filament);

15) децентрализованное хранилище данных, использующее одноранговую сеть компьютеров на Blockchain (компания Storj);

16) оцифровка документов/договоров и свидетельство о праве собственности (компания Colored Coins);

17) цифровая защищенная торговля: право собственности и переводы (компании: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA);

18) перенос денежных средств для сервисов совместных поездок (компания La’Zooz);

19) доказательство собственности для хранилища цифрового контента и доставки (компании Blocktech, Bisantyum, Blockparti, The Rudimrental, BlockCDN);

20) доказательство собственности на модули кода в разработке приложений (компания Assembly).

Приведенные направления применения технологии Blockchain позволяют, уже на данном этапе, решать многие серьезные проблемы в различных сферах Интернет-деятельности. Таким образом, изучение и внедрение технологии Blockchain раскрывает в ближайшем будущем большие перспективы для децентрализации Интернет-сообщества в самых различных отраслях.

УДК 004.412

Обзор методов оценки трудозатрат на предпроектных этапапах при разработке ИУС

Столбовой М.И., аспирант, st.mihail92@gmail.com
Научный руководитель – к.т.н., доц. Мищеряков Ю.В.
Харьковский национальный университет радиоэлектроники, г.Харьков

Предпроектное исследование является стратегической стадией процесса проектирования ИУС, которое проводится в условиях не полной информации при наличии ресурсных и временных ограничений.

Оценка затрат – важная задача, решение которой способствует предварительной оценке возможности создания ИУС и обоснованию целесообразности ее создания.

Для оценки на предпроектных этапах затрат на создание будущей ИУС могут быть применены методы, имеющие достаточный уровень достоверности:

1. Метод функциональных точек – происходит оценка количества функций, приходящихся на реализацию одного функционального требования, с учетом его сложности. В итоге, количество полученных функциональных точек пересчитывается в условные строчки кода или непосредственно в трудозатраты [1].
2. Метод объектных точек – основан на модульном представлении программных систем, с применением обьекто-ориентированого похода. Данный метод достаточно точен, однако его использование оправдано лишь в случаях, когда создается типичная система, или существуют некоторые наработки [2].
3. Метод точек свойств – учитывает не только требования к системе, но и особенности ее реализации. Близок к методу функциональных, с тем отличием, что предусматривает корректирование получаемой оценки с учетом алгоритмической сложности. Наиболее эффективен для систем с незначительным вводом/выводом, но с высокой алгритмической сложностью, таких как математическое ПО, системы дискретного моделирования и т.п. [3].
4. Модель COCOMO II – ориентирована на порционность поступления информации для оценивания, может применятся на протяжении всего периода проектирования; адаптирована к современным методологиям разработки ПО. Модель COCOMO II является самой усовершенствованной технологией, позволяющей рассчитать такое величины как время, затраченное на реализацию проекта, необходимое количество персонала, трудозатраты на IT-проект, а также необходимость в денежных средствах. [2]

Для повышения точности расчета трудозатрат возможно комбинирование данных подходов, используя преимущества данных методов и моделей, что позволит наиболее полно учесть особенности разрабатываемой ИУС.

Список литературы

1. Шафер Д. Управление программными проектами: достижение оптимального качества при минимуме затрат [Текст] / Д. Шафер, Р. Фатрелл, Л. Шафер. - М. : Издательский дом «Вильямс», 2003. - 1136 с.

2. Кульдин, С. П. Генетический подход к проблеме оценки сроков и трудоемкости разработки программного обеспечения с заданными требованиями к качеству [Текст] / Прикладная информатика Выпуск № 5, 2010 – С.30 - 42.

3. Евланов, М. В. Задача оценивания затрат на создание информационной системы [Текст] / М. В. Евланов, Е. И. Соловьева // Materialy X mezinarodni vedecko – prakticka conference « Veda a vznik – 2013/2014». – Dil 34. Moderni informacni technologie. – Praha: Publishing House «Education and Science», 2014. - С. 45 - 48.

УДК 621.391(045)

Оцінка доступності інформаційно-комунікаційних систем з урахуванням різних видів відмов

Терентьєва І.Є., аспірант, i.terentyeva@ukr.net
Науковий керівник – Уланський В.В., д.т.н., професор
Національний авіаційний університет, м. Київ

Задача оцінки доступності інформаційно-телекомунікаційних систем (ІТКС) є актуальною, оскільки підтримка заданого рівня доступності дозволяє забезпечити необхідну якість і обсяг послуг, які надаються.

В сучасних ІТКС використовується цифрова обробка інформації. Аналіз методів контролю цифрових ІТКС показав, що інтервали між періодичним контролем, що проводиться, на стільки малі, що ними можна знехтувати [1], тому будемо вважати, що такі системи охоплені безперервним контролем з кінцевою глибиною тестування.

Проведений аналіз існуючих видів відмов показав, що для цифрових ІТКС характерні раптові відмови, які включають в себе явні та приховані, а також повторювальні відмови і збої, і поступові відмови. Явні відмови діагностуються в тій частині обладнання, яка охоплена постійним контролем, тоді як приховані відмови відбуваються в тій частині обладнання, яка не охоплена контролем. Повторювальні відмови та збої виявляються безперервним контролем або повним додатковим контролем [2]. Поступові відмови проявляють себе при тривалій експлуатації систем і є наслідком деградації параметрів компонентів ІТКС [3].

Як відомо з теорії надійності, найважливішим показником ефективності процесу експлуатації ІТКС є коефіцієнт готовності, який дозволяє оцінити доступність системи в певний момент часу. Однак, наразі відсутні математичні моделі процесу технічного обслуговування (ТО) і оцінки коефіцієнта готовності, які дозволяють врахувати всі види відмов, перераховані вище. Тому результатом проведеного дослідження стала розробка математичних моделей, які дозволяють оцінити середній час знаходження нерезервованих з'ємних модулів (ЗМ) ІТКС в різних станах працездатності та ТО, що дає можливість отримати вирази для розрахунку коефіцієнта готовності ЗМ ІТКС з урахуванням видів відмов та глибини контролю.

Виведено співвідношення, які дозволяють оцінити середній час знаходження ЗМ в досліджуваних станах процесу ТО при довільному розподілі напрацювання ЗМ до відмови на нескінченному інтервалі планування ТО. На підставі цих співвідношень отримано вирази для оцінки коефіцієнта готовності. Проведено дослідження отриманих показників та проілюстровано, що доступність обладнання ІТКС має істотну залежність від інтенсивності повторювальних відмов і глибини контролю.

Таким чином, запропоновані математичні моделі дозволяють вирішити задачу оцінки доступності ІТКМ. Подальшими напрямками даного дослідження є оптимізація різних видів резервування обладнання ІТКМ з метою забезпечення заданого рівня доступності.

Список літератури

1. Иванов А.Б. Контроль соответствия в телекоммуникациях и связи. Часть 1 – М.: Комп. Сайрус системс, 2001. – 376 с.
2. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. - К.: 1995. – 91 с.
3. Грібов В.М. Теорія надійності систем авіоніки: У 2 ч.: Навч. посібник/ В.М. Грібов, Ю.В. Грищенко, А.В. Скрипець, В.П. Стрельніков. – К.: Книжкове вид-во НАУ, 2006. – 324 с.

УДК 004.942:519.2

Лабораторний стенд для досліджень канального та мережного рівнів інформаційно-комунікаційних мереж

Ткаліч О.П., доцент, к.т.н., доцент, tkalich@nau.edu.ua,
Яременко Є.П., студент 3 курсу, yaremenk0.XD@gmail.com
Національний авіаційний університет, Київ

У зв'язку зі стрімким розвитком сучасних інформаційних технологій, зокрема мережевих, зростає необхідність у підготовці висококваліфікованих спеціалістів, здатних проектувати, налаштовувати та обслуговувати комп'ютерні мережі.

В навчальному процесі зазвичай використовують програмне забезпечення для моделювання комп'ютерних мереж, що є невідємною частиною підготовки фахівця. Компютерне моделювання це найкращий та іноді єдиний вихід для набуття студентом теоретичних та практичних навичок в роботі з мережами, але не кожене програмне забезпечення дозволяє провести досліджень над змодельованою мережею. Також моделювання не дає можливості студенту провести діагностування мережі на фізичному рівні, знайти недоліки в обжимі кабелів та монтажі пасивного обладнання.

На нашу думку, моделювання необхідно закріплювати на практиці, Вам пропонується розглянути можливості лабораторного стенду, який використовується в навчальному процесі кафедри телекомунікаційних систем Національного авіаційного університету.

На рис. 1 представлено структурну схему лабораторного стенду.

Стенд складається з наступних мережевих пристроїв:

1. Маршрутизатор (М) TP-Link TL-R860;
2. Комутатори (К) TP-Link TL-SF1005D (2 штуки);
3. Патч-панель;
4. Комунікаційна розетка.
5. Патч-корди та кабель «кручена пара»

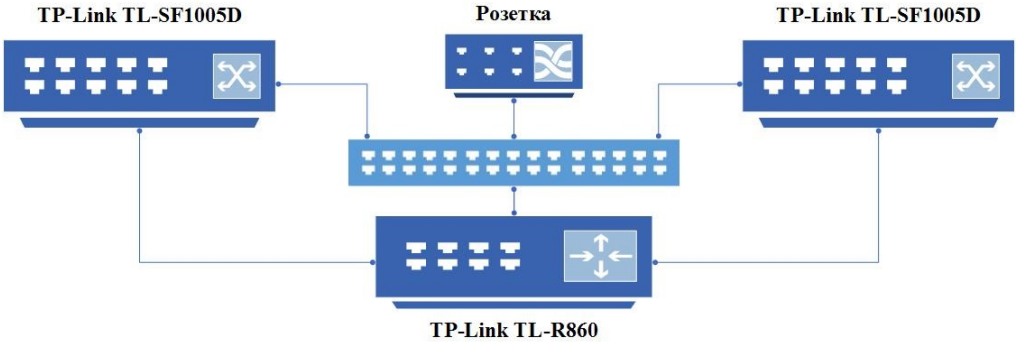


Рисунок 1 – Структурна схема лабораторного стенду

Опис стенду

Стенд є набором активного та пасивного обладнання для побудови структурованих комп'ютерних мереж зібраного на площині 120*80 сантиметрів (габарити можна зменшити) та є цілісним. Все активне комутаційне обладнання підєднано до патч-панели кабелями «кручена пара», що дозволяє підвищити зносостійкість портів активних пристроїв. Кожен порт патч-панели пронумеровано та має відповідне підключення до певного порта комутатора/маршрутизатора/розетки що імітує роботу в серверній з комутаційної стійкою.

Представлений стенд надає можливість студентам створювати однорангові та клієнт-серверні архітектури комп'ютерні мережі. Лабораторні роботи, які студент виконує на даному стенді:

Обжим кабеля та первірка на правильність обжиму за допомогою тестерів або комп’ютерів (ПК), монтаж патч-панелі та перевірка її працездатності;

Налаштування однорангової мережі ПК-ПК та перевірка її роботи;

Налаштування мережі ПК-К-ПК;

Налаштування ПК-К-К-ПК, та підключення до мережі декількох активних пристроїв для збільшення навантаження в мережі;

Дослідження характеристик мережі на канальному рівні за допомогою аналізатору трафіка Wireshark;

Дослідження функціонального призначення команд командної строки;

Перевірка формувань ARP-таблиць;

Дослідження затримок в мережі при збільшенні/зменшенні навантаження на комунікаційні вузли;

Дослідження затримок при передачі різної кількості запитів різної довжини;

Дослідження затухань в каналі зв’язку при різних довжинах кабелю;

Налаштування ПК-М-ПК та ПК-К-М-К-ПК для досліджень протоклів мережевого рівня;

Повне налаштування маршрутизатора відповідно до його функціоналу та дослідження його можливостей.

Перевагами стенду є можливість одночасної роботи студентів над виконанням різних лабораторних робіт. Зовнішній вигляд стенду представлено на рис. 2.

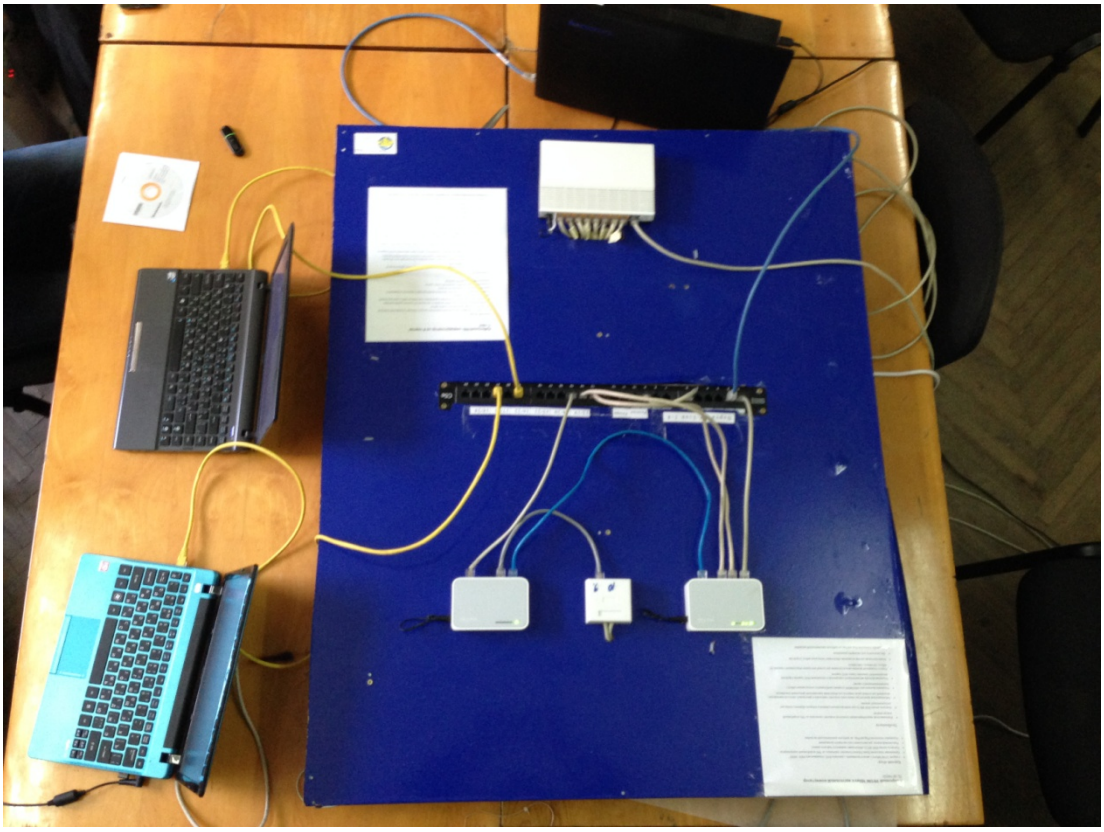


Рисунок 2 – Зовнішній вигляд лабораторного стенду.

Висновки. Таким чином, даний лабораторний стенд, дозволяє досліджувати характеристики канального та мережного рівнів проводити лабораторні роботи студентами ВНЗ, які вивчають дисципліни пов’язані з інформаційно-комунікаційними мережами.

УДК 004.415.52

Оцінка вимог до програмних засобів за критерієм тестопридатності

Улічев О.С., аспірант
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Тестування є невід'ємним процесом життєвого циклу програмного забезпечення, являє собою трудомісткий процес, що вимагає залучення як трудових так і часових ресурсів. Ґрунтовні дослідження і розроблені методи тестування не дають можливості повністю виключити помилки, в наслідок цього помилки в програмному забезпечені присутні на етапах впровадження і використання. Досліджуючи еволюцію підходів до тестування, можна помітити тенденцію – тестування завжди намагаються провести якомога раніше з метою запобігти можливих помилок на наступних стадіях проекту. Сучасна наукова думка намагається знайти такий підхід, який би забезпечував можливість тестування навіть раніше самого проекту, тобто на етапі виникнення ідеї. Уваги, в цьому сенсі, набуває критерій тестопридатності. Важливість і актуальність дослідження підтверджується, в тому числі, аналізом останнього стандарту [2]. Так в розділі 7 (процеси життєвого циклу програмних засобів) окремим пунктом виписано: «перевірка системних вимог на коректність і тестованість».

Вимогами (requirements) називають опис функціональних можливостей і обмежень, що накладаються на програмний продукт. Виділяють початкові вимоги (вимоги замовника) і деталізовані вимоги (вимоги розробника). Які в сукупності утворюють програмну специфікацію.

За визначенням МакКоннелла «testability» є ступінь можливості тестування програми на системному і модульному рівнях та перевірки програмного продукту на відповідність вимогам (валідності) [1]. Виходячи з означення, оцінка рівня тестування (надалі будемо використовувати термін тестопридатність) є сутністю, що пов'язує поняття: валідація, програмна специфікація, стратегія тестування і тестування безпосередньо.

Мета дослідження: покращення результатів тестування за рахунок вибору тестів на основі аналізу вимог до програмного забезпечення та оцінки критерію тестопридатності вимог до ПЗ.

Аналіз розподілу помилок на різних стадіях проекту приводиться в працях [1,3,4], зокрема в праці Гласса [3] вказано, що на стадіях впровадження та експлуатації програмного забезпечення залишається близько 50% помилок. Єдиною причиною цього вбачається неправильність стратегії тестування та підбір тестів невідповідних до задачі. В тій же праці наводиться статистика – 64% помилок проекту закладаються на рівні аналізу.

Ефективний аналіз вимог має виявити проблемні ситуації і передбачити шляхи їх подолання на до проектному етапі.

Для вимог до програмного продукту стандартом [6] передбачено наступний перелік критеріїв: а) коректність; б) однозначність; в) повнота; г) несуперечливість; д) упорядкованість по важливості і стабільності; е) тестопридатність; ж) можливість модифікації; з) можливість відстеження.

Вимога в цілому є тестопридатною тоді і тільки тоді, коли кожна з складових його елементарних вимог є тестопридатною. Елементарна вимога вважається тестопридатною тоді і тільки тоді, коли існує кінцевий фінансово ефективний процес, за допомогою якого людина або машина можуть визначити, що розроблена програмна система дійсно задовольняє даній вимозі [6]. Виходячи з цього можна запропонувати планування тестів вже на етапі аналізу вимог за критерієм тестопридатності, при розробці тестів необхідно передбачити тести всіх складових елементарних вимог (ЕВ). В найпростішому випадку результат оцінки може набувати двох значень: ЕВ не тестопридатна – необхідна корекція або уточнення вимоги, ЕВ тестопридатна – зафіксувати в тестовому наборі тест для даної ЕВ. Бажано щоб кожна деталізована вимога могла бути простеженою і в прямому, і в зворотному напрямку. Рисунок 1 демонструє переваги жорсткої відповідності між кожною окремою функціональною вимогою, частиною проектного рішення, що

реалізує вимогу і відповідною частиною програмного коду. Вони пов'язані з тестом реалізації вимоги.

Простеження не функціональних вимог суттєво складніше, в більшості випадків не можна встановити чіткої взаємної відповідності «1 не функціональна вимога» – «1 елемент програмного коду».

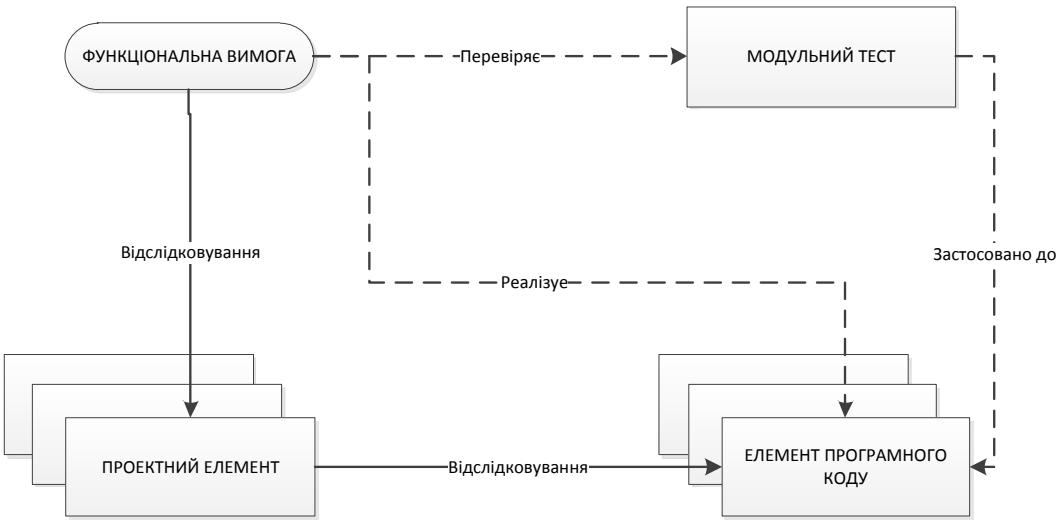


Рисунок 1 - Відстеження і тестування функціональних детальних вимог до ПЗ

З огляду на проведені дослідження можна зробити наступні висновки:

- Тестопридатність є відносною характеристикою, що визначає співвідношення між початковими вимогами до програмного забезпечення їх деталізацією і методами майбутнього тестування.
- Тестопридатність вимог однозначно має взаємозв’язок з подальшими підходами та стратегією тестування.
- Процес оцінки тестопридатності вимог, декомпозиція вимоги на складові елементарні вимоги є основою для складання базового обов’язкового набору тестів.
- Оцінки тестопридатності, на ряду з іншими критеріями оцінки вимог до програмного забезпечення, визначають необхідність внесення коректив з метою уточнення і конкретизації проблемних моментів в вимогах до програмного засобу.

Література:

1. Макконнелл С. Совершенный код. Мастер класс / Макконнелл С. [пер. с англ.] - М.: Издательство «Русская редакция», 2010. — 896 с.

2. ISO/IEC 12207:2008 "System and software engineering - Software life cycle processes"

3. Гласс Р. Креативное программирование / Роберт Гласс. [пер. с англ.] — СПб.: Символ, 2009. — 352 с.

4. Майерс Г. Надежность программного обеспечения / Гленфорд Дж. Майерс [пер. с англ.] - М.: Мир, 1980. — 360 с.

5. Д. Леффингуэлл Принципы работы с требованиями к программному обеспечению. Унифицированный поход./ Д. Леффингуэлл, Д. Уидриг –М.: Вильямс, 2002, - 448 с.

6. EEE 830-1998 Методика составления спецификаций и требований к программному обеспечению

УДК 004.5

Веб-портал університетського бізнес-центру підтримки новостворених ІТ-компаній

Хворостенко Р.Ю., студент 4-го курсу, incommoditer@gmail.com
Науковий керівник – Савельєв М.В., старший викладач
Національний технічний університет України "КПІ" Славутицька філія, м. Славутич

Вищі навчальні заклади України щорічно випускають близько шістнадцяти тисяч спеціалістів в сфері ІТ, але тільки приблизно третина з них працюють по спеціальності, оскільки випускники не відповідають вимогам ринку [4]. Це пов'язано з тим, що вищі навчальні заклади України орієнтуються на випуск спеціалістів широкого профілю, які не мають досвіду в промисловій розробці програмного забезпечення і вимагають додаткової підготовки на підприємствах.

Вдалим досвідом в економічно розвинутих країнах стало створення бізнес-центрів при університетах, які займаються створенням нових компаній або під ідею, або під проект, коли університет виконує замовлення підприємств. При цьому участь студентів в даній роботі сприяє підвищенню професійної кваліфікації.

В Україні питанню формалізації співпраці університеті і промисловості присвячені статті В.С. Харченка, В.В. Скляра [1,2], а також роботи В.В.Литвинова та ін. [4], де був проаналізований перший практичний досвід кооперації університетів і промисловості.

Робота зазначених бізнес-центрів повинна бути підтримана різноманітними інструментами. В роботах [3, 4] зазначалося, що одним з таких інструментів повинен стати веб-портал, центр об'єднання і його адміністративно-наглядову раду, створені компанії і їх проекти. Питанню створення такого веб-порталу присвячена дана стаття.

Метою роботи вважається розробка веб-порталу бізнес центру при університеті для підтримки новостворених ІТ-компаній. Тому в перелік основних завдань даної роботи входить виявлення, аналіз і формулювання вимог до даного веб-порталу, а також побудова його ескізної архітектури. З метою вирішення даних завдань необхідно побудувати модель предметної області, взаємодії веб-порталу з його користувачами. Та запропонувати архітектуру веб-порталу. Та запропонувати архітектуру веб-порталу.

Після порівняльного аналізу основних сучасних технологій розробки веб-додатків було вирішено розробляти веб-портал завдяки фреймворку Django, який зумовлює використання мови програмування Python. Цей вибір пов'язаний з тим, що Django призначений для швидкої розробки відкритих модульних веб-додатків різної складності. Мова Python пропонує використання методів інтеграції різних модулів написаних на різних мовах програмування (інтеграція з мовою Java, C++, C). Також Python дозволяє інтегрувати веб-додаток Django з веб-додатками для керування проектами і задачами, такими як Redmine і Jira. Всі ці переваги відповідають вимогам ЧНТУ до веб-порталу бізнес-центру. А саме інтеграції різних модулів на різних мовах програмування, та інтеграції з системами керування проектами і задачами Redmine і Jira. В якості бази даних було обрано безкоштовну систему керування базами даних PostgreSQL, яка надає весь спектр можливостей необхідних для розробки даного програмного продукту. Отриманий прототип веб-порталу має вигляд (рис.1):

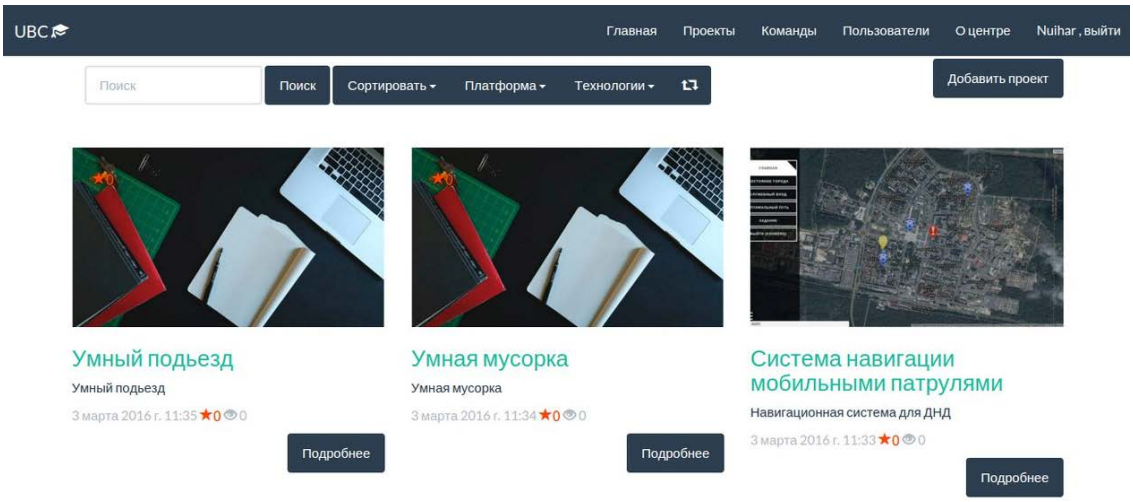


Рисунок 1 – Прототип веб-порталу університетського бізнес-центру

Висновки. Таким чином, зазначений веб-потрал має дуже вагоме практичне значення: реалізує зв'язок між новоствореними компаніями, бізнес-цетром і підприємствами; автоматично робить оцінку компетенції новоствореної ІТ-компанії; реалізує процес підтримки новостворених ІТ-компаній бізнес центром. На даний момент, вдалося виявити основні вимоги до веб-порталу, побудувати модель предметної області, побудувати модель взаємодії веб-порталу з користувачами та почати розробку зазначеного веб-порталу. Веб-портал розробляється з використанням найсучасніших технологій розробки програмного забезпечення, що дозволяє використовувати найкращі практики останніх років.

Список літератури

1. Харченко, В.С. Концепция и модели взаимодействия университетской науки и ИТ–индустрии: S2B–B2S [Текст] / В.С. Харченко, В.В. Скляр // КАРТБЛАНШ. – Вип. 8–9. –2012. - С.45-52

2. Харченко, В.С. Кооперация университетов и индустрии: S2B–B2S [Текст] / В.С. Харченко, В. В. Скляр // КАРТБЛАНШ. – Вип. 3-4. –2014. - С.43-49

3. O.Starov, V.Kharchenko, V.Sklyar and N.Khoklienkov, Advanced Spin-off model of UIC. University-Industry Interaction Conference, http://www.university-industry.com, Amsterdam, May 2013

4. Lytvynov V.V., Kharchenko V.S., Lytvyn S.V, .Saveliev M.V., Trunova E.V., Skiter I.S. Tool-Based Support of University-Industry Cooperation in IT-Engineering. - Ministry of Education and Science of Ukraine, Chernihiv National University of Technology. 2015.

УДК 004.89:004.6

Використання Django framework для створення сайту рекомендаційної мережі із застосуванням колаборативної фільтрації

Яровенко І.В., студент, yarovenko.13@gmail.com
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Останнім часом прикладні програми пройшли шлях від маленьких та порівняно простих додатків до великих та складних систем. Але з часом такі рекомендації стали витісняти цільовими пропозиціями: користувачам не просто рекомендують популярні продукти, а ті продукти, які напевно сподобаються саме їм. По мірі збільшення кількості пропозицій стає менш практично опитувати невеликі групи людей, оскільки вони можуть не знати про всі існуючі варіанти. Тому, використовують колаборативну фільтрацію.

Рекомендаційна система – підклас системи фільтрації інформації, яка будує рейтинговий перелік об'єктів (фільми, музика, книги, новини, веб-сайти), яким користувач може надати перевагу. Для цього використовується інформація з профілю користувача.

Існують дві основні стратегії створення рекомендаційних систем: фільтрація вмісту і колаборативна фільтрація.

При фільтрації вмісту створюються профілі користувачів і об'єктів.

Профілі користувачів можуть містити демографічну інформацію або відповіді на певний набір питань.

Профілі об'єктів можуть містити назви жанрів, імена акторів, імена виконавців або якусь іншу інформацію в залежності від типу об'єкта.

При колаборативній фільтрації використовується інформація про поведінку користувачів у минулому – наприклад, інформація про придбання або оцінки. В цьому разі не має значення, з якими типами об'єктів ведеться робота, але при цьому можна брати до уваги неявні характеристики, які складно було б врахувати при створенні профілю. Основна проблема цього типу рекомендаційних систем – «холодний старт»: відсутність даних про користувачів чи об'єкти, які нещодавно з'явились у системі.

Колаборативна фільтрація – це один з методів побудови прогнозу в рекомендаційних системах, який використовує відомі переваги (оцінки) групи користувачів для прогнозування невідомих переваг іншого користувача. Його основне припущення полягає в наступному: ті, хто однаково оцінювали будь-які предмети в минулому, схильні давати схожі оцінки інших предметів і в майбутньому. Наприклад, за допомогою колаборативної фільтрації музичний додаток здатний прогнозувати, яка музика сподобається користувачеві, маючи неповний список його переваг (симпатій і антипатій). Прогнози складаються індивідуально для кожного користувача, хоча використовувана інформація зібрана від багатьох учасників. Тим самим колаборативна фільтрація відрізняється від більш простого підходу, дає усереднену оцінку для кожного об'єкта інтересу, наприклад, що базується на кількості поданих за нього голосів. Дослідження в даній області активно ведуться і в наш час, що також обумовлюється і наявністю невирішених проблем в колаборатівній фільтрації.

У розробленій системі використано наступний алгоритм колаборативної фільтрації:

$$r_{u,i} = k \sum_{u' \in U} sim(u,u') r_{u',i}$$

де функція sim – обрання міри схожості двох користувачів, U – кількість користувачів, r – виставлена оцінка, k – нормований коефіцієнт, який обчислюється за формулою:

$$k = 1 / \sum_{u' \in U} |sim(u,u')|$$

Для розробки сайту рекомендаційної мережі із застосуванням колаборативної фільтрації було обрано мову програмування Python.

Python чудово підходить для швидкої розробки. Код однакової функціональності на Python може займати в декілька разів менше місця ніж код на C++ чи Java. До того ж Python є інтерпретованою мовою, а тому не потрібно витрачати час на чергову компіляцію, щоб протестувати код після чергового виправлення.

Для Python існує величезна кількість середовищ розробки (IDE). Для даної роботи було обрано високорівневий Python-фреймворк Django.

Django (Джанго) – високорівневий відкритий Python-фреймворк для розробки веб-систем. Названо його було на честь джазмена Джанго Рейнхардта (відповідно до музичних смаків одного зі засновників проекту).

Сайт на Django будується з однієї або декількох частин, які рекомендується робити модульними. Це одна з істотних архітектурних відмінностей цього фреймворку від деяких інших (наприклад Ruby on Rails).

Архітектура Django подібна на «Модель-Вид-Контролер» (MVC). Однак, те що називається «контролером» в класичній моделі MVC, в Django називається «вид» (англ. view), а те, що мало б бути «видом», називається «шаблон» (англ. template). Таким чином, MVC розробники Django називають MTV («Модель-Шаблон-Вид»).

Початкова розробка Django, як засобу для роботи новинних ресурсів, досить сильно позначилася на його архітектурі: він надає ряд засобів, які допомагають у швидкій розробці веб-сайтів інформаційного характеру. Так, наприклад, розробнику не потрібно створювати контролери та сторінки для адміністративної частини сайту, в Django є вбудований модуль для керування вмістом, який можна включити в будь-який сайт, зроблений на Django, і який може керувати відразу декількома сайтами на одному сервері. Адміністративний модуль дозволяє створювати, змінювати і вилучати будь-які об'єкти наповнення сайту, протоколюючі всі дії, а також надає інтерфейс для управління користувачами і групами (з призначенням прав).

У дистрибутив Django також включені програми для системи коментарів, синдикації RSS і Atom, «статичних сторінок» (якими можна управляти без необхідності писати контролери та відображення), перенаправлення URL та інше.

Деякі можливості Django:

– вбудований інтерфейс адміністратора, з уже наявними перекладами на більшість мов;
– диспетчер URL на основі регулярних виразів;
– розширювана система шаблонів з тегами та наслідуванням;
– система кешування;
– інтернаціоналізація;
– «generic views» - шаблони функцій контролерів;
– авторизація та аутентифікація, підключення зовнішніх модулів аутентифікації: LDAP, OpenID та ін.;
– система фільтрів («middleware») для побудови додаткових обробників запитів, наприклад включені в дистрибутив фільтри для кешування, стиснення, нормалізації URL і підтримки анонімних сесій;
– бібліотека для роботи з формами (наслідування, побудова форм за існуючою моделлю БД);
– вбудована автоматична документація по тегам шаблонів та моделям даних, доступна через адміністративний застосунок;

Різні компоненти фреймворку між собою пов'язані слабо, тому достатньо будь-яку частину замінити на аналогічну.

З вище перерахованого можна зробити висновок, що обраний Python-фреймворк Django підходить для створення рекомендаційної мережі, а використання колаборативної фільтрації дозволить керувати мережевою аудиторією за допомогою цілеспрямованої фільтрації інформації та вироблення рекомендацій для нових посилань, статей і т.д.

Секція 3.
Інтелектуальні системи та штучний інтелект

УДК 004.822

Модель інтелектуальної системи формування вимірювальних баз знань

Асабашвілі С.Д., аспірант, sulico@mail.ua
Науковий керівник – Волков С. Л., к. т. н., доцент
Одеська державна академія технічного регулювання та якості, м. Одеса

Вимірювальні завдання, що забезпечують отримання вимірювальної інформації необхідної для функціонування складних технічних систем, пов'язані із отриманням і інтерпретацією різноманітних за формою та структурою експериментальних даних. Забезпечення об’єктивності, достовірності та високої швидкості отримання результатів вимірювань стримуються складністю формалізації різнорідної інформації, за допомогою класичних математичних методів та моделей та значними потужностями необхідних технічних засобів потрібних для реалізації цих моделей. Така ситуація зумовила появу нового напряму інформаційно-вимірювальної техніки – інтелектуальних інформаційно-вимірювальних систем. Який орієнтований на ефективне вивчення властивостей складних об’єктів і середовища взаємодії цих об'єктів, виявлення взаємозв'язків між ними шляхом узагальнення всіх видів апріорної і експериментальної інформації з метою генерації нових знань.

Така генерація пов’язана з процесом їх опису. Апріорні знання, крім формалізованого вигляду, можна описати і за допомогою мов штучного інтелекту, які дозволяють не тільки відображати дані в різних моделях уявлення апріорних знань, а й працювати з цими моделями. Такими мовами, насамперед, є LISP і PROLOG. У випадку коли можливостей мов штучного інтелекту недостатньо, застосовуються мови традиційного програмування, які дозволяють використовувати комп’ютерно-інтегровані інтелектуальні підсистеми (наприклад, інтегровані експертні системи).

Для задач метрологічного аналізу результатів вимірювання (проведеного експерименту) виникає необхідність в організації баз даних, які містять: вхідні параметри, види вимірювальних процедур, моделі модулів вимірювальних процедур, моделі метрологічних характеристик, моделі оцінок метрологічних характеристик та інших складових. Така сукупність взаємопов'язаних послідовностей апріорної і апостеріорної інформації метрологічного експерименту з необхідною оцінкою достовірності в літературі носить назву вимірювальних знань, які налічують десятки моделей та методів формування.

На рис. 1 представлена структурна СУБД вимірювальних знань. Дані зберігаються в базах знань і використовуються при вирішенні задач експертною системою. Представлена СУБД являє собою комплекс взаємопов'язаних модулів, які дозволяють системі ефективно і з достатньою точністю вирішувати наступні поставлені завдання:

1. Формувати базу початкових вимірювальних знань.
2. Вводити нові вимірювальні дані, перетворювати їх в знання шляхом знаходження нових залежностей і виявлення нових закономірностей, адаптувати систему в разі потреби на підставі цих знань.
3. Зберігати вимірювальні знання в базі даних (БД) для використання і оптимізації по якомусь критерію або параметру.
4. Забезпечувати організацію консультуючої системи.
5. Забезпечувати організацію експертної системи, що дозволяє за допомогою графічного інтерфейсу вирішувати завдання.

В представленій базі знань мовою програмування є PROLOG з включеними модулями RAD або Python, що дає змогу реалізації графічного інтерфейсу, який забезпечує отримання вимірювальної інформації та консультації експертної системи, введення/виведення вимірювальних даних в/з програми використовується підсистема графічного інтерфейсу. За основу інтерпретатора

PROLOG узятий SWI-PROLOG, який відрізняється якістю опрацювання і наявністю розвитого інтерфейсу доступу до БД.

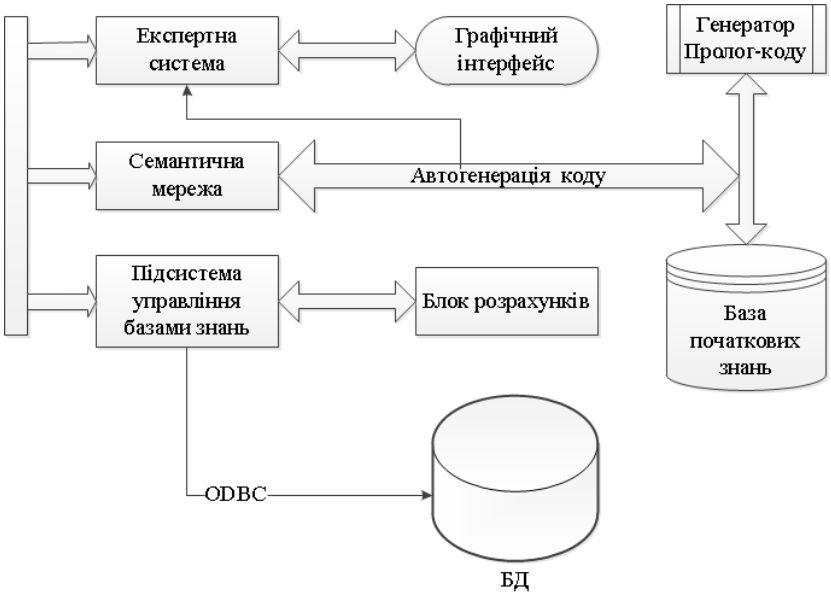


Рисунок 1 – Схема взаємодії системи формування вимірювальних баз знань

Користувач отримує консультацію експертної системи у вигляді рекомендацій, шляхом постановки йому питань або на основі отриманої вимірювальної інформації. При наявності неповних або помилкових вимірювальних даних експертна система може видати список помилок. Важливою особливістю експертної системи є те, що користувач може отримати не тільки консультації, а і всі знання, що зберігає система з урахуванням його прав доступу. Для реалізації цих функцій даний модуль пов'язаний с модулем підсистеми управління базами знань і з модулем семантичної мережі.

Формування структури бази даних здійснюється на основі загальної послідовності процесів вимірювання і має рекомендовану найпростішу структуру, що складається з наступних моделей та відповідних їм множин вхідних даних:

Модель міри метрологічної достовірності{Вхідний вплив; Фізична природа сигналу {Звукова хвиля, Світлова Хвиля, Електромагнітна Хвиля}; Математична структура сигналу {Частота сигналу, Вид функції, Вид розподілу}};

Модель процедури перетворення {Тип процедури {Тип 1 … Тип n}; Вид МХ {Лінійна, Нелінійна}; Номенклатура модуля{Модулі фільтрації{Перетворення Фур'є, Обрізання частот, Зворотне перетворення Фур'є}; Модулі квантування {Дискретизація, Квантування, Зчитування, Перетворення, Масштабування, Перенесення}}};

Модель методу оцінки достовірності {Тип методу {Імітаційне моделювання, Метрологічний експеримент, Аналітичний розрахунок}};

Модель послідовності перетворень{Вид повної похибки; Вид метрологічної похибки; Рівняння вимірювань; Перетворення {Форма перетворень {Аналогова, Цифрова}; Перетворення нормалізації {Зворотне, Пряме}}};

Модель оцінки достовірності{Метрологічна характеристика результату{Математичне очікування оцінки результату, Середньоквадратичне відхилення оцінки}}.

Список літератури

1. Раннев Г.Г. Интеллектуальные средства измерений / Г.Г. Раннев. – М.: Академия, 2011. – 272 с.

2. Брусакова И.А. Модели представления измерительных знаний в информационно-измерительных технологиях: учебное пособие / И.А. Брусакова. – СПб.: Изд-во СПбГЭТУ, 2002. – 352 с.

3. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский. – СПб.: Питер, 2000. – 384 с.

УДК 681.516.54 / 551.521.31

Прийняття рішень в умовах вибору оптимального складу системи

Голик О.П., доцент, кандидат технічних наук, доцент, dego@ukr.net,
Жесан Р.В., доцент, кандидат технічних наук, доцент, zherom@ukr.net
Кіровоградський національний технічний університет, м. Кіровоград

Існуючі АСК автономного енергопостачання (АЕП) на основі відновлюваних джерел енергії (ВДЕ) не завжди можуть адекватно реагувати на порушення та збої в процесі керування системою. Пояснюється це тим, що в системі може бути не враховано цілий ряд неконтрольованих параметрів, а це, в свою чергу, суттєво змінює режим роботи системи та погіршує показники якості.

Новим напрямком у розвитку теорії та практики автоматизованих систем керування (АСК) об'єктами в умовах невизначеності є використання інтелектуальних систем, зокрема інтелектуальні підсистеми підтримки прийняття рішень (ІППРР).

ІППРР повинна базуватись на алгоритмах автоматичної корекції для коригування значень параметрів системи у разі виникнення порушень та збоїв в процесі енергопостачання. Від ефективної роботи алгоритмів залежить швидкість виявлення причини порушення. Складність прийняття рішення при цьому зумовлена тим, що зміна в роботі системи може відбутись під впливом різних слабоформалізованих факторів, а підтримання показників якості процесу необхідно виконувати зміненням різних взаємопов'язаних параметрів. Розв'язання цієї задачі є актуально новою науковою проблемою.

Припустимо, що система характеризується *m* вхідними (незалежними) векторами-змінними і одним вихідним (залежним) вектором-змінною. Вхідні змінні мають стохастичний характер. Система повинна бути побудована таким чином, щоб необхідні процеси (стабілізації, перетворення. перерозподілу параметрів) впливали згідно із певним законом на кожний вхід у відповідний час для досягнення бажаного результату. У загальному вигляді наша АСК може бути зображена у вигляді, представленому на рис. 1 [1].

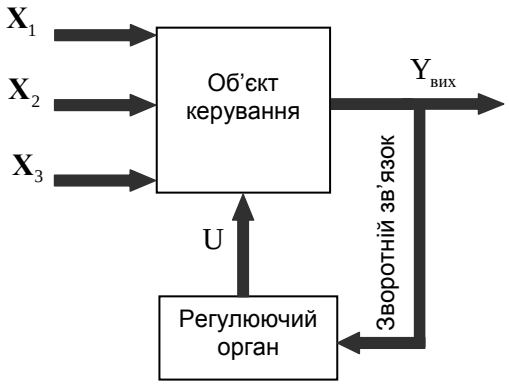


Рисунок 1 – АСК АЕП у загальному вигляді

$\mathbf{X_1}$ – вектор навантаження системи (інформація, енергія); $\mathbf{X_2}$ – вектор впливів зовнішнього оточуючого середовища (сукупність факторів та явищ, які діють на процеси системи і не піддаються прямому керуванню зі сторони споживача); $\mathbf{X_3}$ – вектор, який задає закони організації та функціонування параметрів системи, мету, граничні умови та ін; $\mathbf{Y_{вих}}$ – вектор вихідних координат (є продуктом або результатом діяльності системи). На виході АСК АЕП повинна задовольняти ряду критеріїв, найважливішими з яких є стабільність та надійність роботи; **U** - вектор керуючого впливу.

За допомогою зворотного зв'язку інформація з виходу системи об'єкта керування передається на регулюючий орган. Потім цей сигнал, який має інформацію про виконані дії,

порівнюється з сигналом, який задає навантаження в системі. У випадку виникнення розузгодження між фактичним та запланованим станом роботи, виконуються дії щодо усунення цього розузгодження.

Невизначеність в даній системі поділяється на два різновиди [2]. По-перше – статистична невизначеність, яка обумовлена випадковістю. Наприклад, невизначеність появи або інтенсивність того чи іншого джерела енергії. По-друге – дійсна невизначеність, коли невідомо, який з відомих або невідомих факторів (законів) впливає в даному конкретному випадку на випадкові події. Наприклад несправність одного з перетворювачів енергії, непередбачені стихійні лиха, різке зростання навантаження в системі. Іншими різновидами невизначеності є: неможливість врахування всіх факторів, які впливають на прийняття рішень, складності їх кількісної оцінки.

Дерево рішень – схематичне представлення проблеми ПР. Використовується для вибору найкращого напрямку дій з тих варіантів, що існують. На рис. 1 наведено дерево рішень для прийняття рішення щодо керування АСК АЕП в умовах ризику [3].

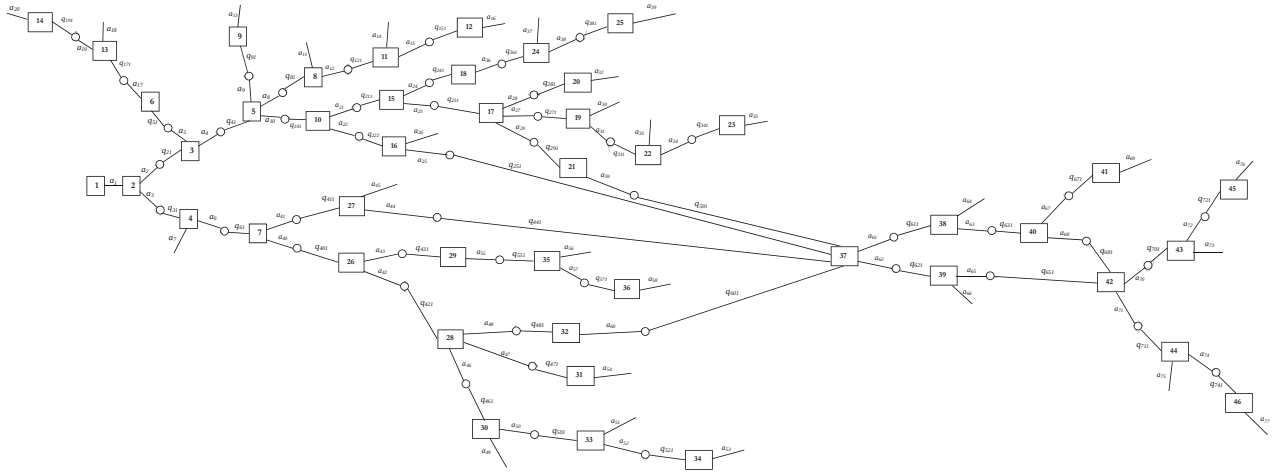


Рисунок 1 – Структурне зображення процесу АЕП в задачі вибору оптимального керування АСК АЕП

На основі даної структури в подальшому буде побудована функція належності, за допомогою якої можна буде обирати оптимальний склад системи енергопостачання.

Висунута гіпотеза потребує подальшої перевірки на основі комп’ютерного моделювання і експериментальних досліджень.

Застосування функцій належності в умовах нечіткої інформації дозволяє формалізувати якісні характеристики потенційного збитку, що можливий у результаті вибору комбінацій енергетичних потоків; й імовірності виникнення небажаних наслідків, яким відповідає певний збиток, для конкретної ситуації прийняття рішень.

Список літератури:

1. Голик О.П. Оптимізація задачі керування енергозабезпеченням автономних споживачів в умовах невизначеності / О. П. Голик, Р. В. Жесан, І.А. Березюк, М.С. Мірошніченко // Сборник статей научно-информационного центра «Знание» по материалам IX международной заочной научно-практической конференции: «Развитие науки в XXI веке» г. Харьков: сборник со статьями (уровень стандарта, академический уровень). – Д. : научно-информационный центр «Знание», 2015. – Ч. 1., С. 77-81. 188с.

2. Осадчий С.І. Модернізована оптимальна робастна багатовимірна фільтрація стаціонарних випадкових корисних сигналів / С.І. Осадчий, О.Я. Кузнєцова, В.О. Зубенко, О.П.Голик //Наукоємні технології. – 2015. – Т. 27. – №. 3. – С. 229-232.

3. Голик О.П. Пошук оптимальних рішень щодо вибору джерел енергії, які доцільно використовувати для автономного енергопостачання / О.П. Голик// Відновлювана енергетика. – 2013. - № 2. – С. 24-27.

УДК 004.8

Експертна система, як спосіб технічної діагностики інтегрованої інформаційної системи

Коваленко А.С., асистент, annasun911@gmail.com
Лісовий В.А., студент 2 курсу, matr1x7772@gmail.com
Кіровоградський національний технічний університет, м. Кіровоград

Інтегрована інформаційна система (ІІС) є складною системою, реалізованою за допомогою технічних засобів, телекомунікаційних та комп'ютерних мереж і відповідного програмного забезпечення [1]. Складність алгоритмів управління мережею і специфіка взаємодії об'єктів мережі значно ускладнюють рішення завдань діагностики і відновлення мережі після збоїв. Крім того, в процесі функціонування мережі можуть виникати різні непередбачувані ситуації, що призводять до аварійного стану на окремих ділянках мережі або в усій мережі в цілому. Ці та інші пов'язані з ними проблеми викликають необхідність автоматизації діагностики стану ІІС та її об'єктів.

Через велику кількість об'єктів діагностики, складності і некоректності протоколів різних рівнів завдання технічної діагностики (ТД) ІІС є таким, що погано формалізується. Тоді традиційні способи технічної діагностики (апаратний і функціональний контроль) будуть малоефективними. Найбільш перспективним підходом до рішення цієї задачі є розробка і створення експертної системи (ЕС) ТД ІІС, оскільки останнім часом з розвитком теорії штучного інтелекту їх все частіше стали використовувати для вирішення таких складних завдань [2].

Метою даної роботи є розробка структури ЕС, яка б задовольняла вимоги ІІС, щодо ефективного технічного діагностування.

Така система ТД повинна за інформацією, що поступає від ІІС, оцінювати поточний стан мережі та її об'єктів, здійснювати пошук несправностей, прогнозувати подальший розвиток ситуації на об'єктах діагностики, представляти отримані результати в зручній для розуміння оператором формі. Розвиток ІІС йде шляхом ускладнення об'єктів мережі, протоколів їх функціонування з метою підвищення ефективності і надійності мережі. Це призводить до підвищення надійності роботи і ускладнення пошуку несправностей через ідентичність симптомів.

Було встановлено та доведено, що ЕС з традиційною структурою не підходить для діагностики ІІС через погану формалізуємість знань цієї предметної області.

З вимог, що пред'являються до ЕС ТД витікає, що, окрім діагностики, стану мережі, необхідно оцінювати ефективність роботи самої ЕС і, якщо необхідно, довчити систему. Система ТД ІІС повинна працювати в реальному масштабі часу.

Тому для підвищення ефективності її роботи необхідно використовувати запропоновану в [3] схему ("вежу" числень). Тоді структура ЕС ТД стане ієрархічною. На першому рівні ієрархії вирішуватимуться завдання ТД ІІС, а на другому – періодично оцінюватиметься якість діагностики мережі і, якщо необхідно, відбуватиметься навчання модулю першого рівня.

Виходячи з проведених вище міркувань, ЕС ТД ІІС можна представити у вигляді сукупності модулів першого рівня, додаткових і другого рівня. Структура ЕС ТД ІІС матиме вигляд, показаний на рис. 1.

Алгоритм функціонування якої буде наступним. Інформація, що поступає від ІІС і її об'єктів в певні проміжки часу, зберігається в модулі БД. За поточними даними з БД і на підставі інформації з БЗ модуль отримання результату визначає поточний і прогнозує майбутній стан ІІС та її об'єктів. Використання процесуальних міркувань при прийнятті рішення дозволяє ЕС вирішувати завдання ТД ІІС в умовах неповноти і суперечності БЗ, видавати користувачеві наближені відповіді, якщо на підставі отриманої інформації неможливо отримати точну відповідь. Якщо отриманої інформації недостатньо для вирішення завдань ТД, то ЕС має можливість звернутися до інших видів знань (функціональних, структурних, евристичних, історичних). Використання знань про особливості побудови і функціонування ІІС та історичних знань дозволяє

ЕС "моделювати" процеси, що протікають на ІІС. Потім отримане рішення задачі ТД ІІС поступає в модуль візуалізації та пояснення, де воно обґрунтовується за допомогою аргументів, які використовувалися при рішенні задачі ТД ІІС. Після цього рішення задачі ТД ІІС разом з поясненнями за допомогою модуля діалогу видається користувачеві.

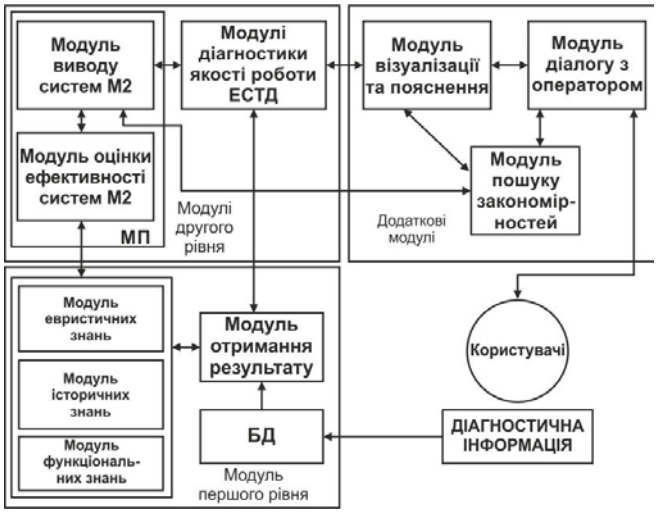


Рисунок 1 – Модульна структура ЕС ТД

Результати роботи ЕС ТД періодично оцінюються в модулі діагностики якості функціонування, де приймається рішення про необхідність внесення змін до роботи ЕС. Під змінами в роботі ЕС ТД будемо розуміти заміну поточної системи на нову, більш ефективну. Для видозміни поточної системи або для пошуку нової призначений модуль пошуку ефективних систем. Якщо модуль пошуку (МП) не знайшов ефективнішої системи або модифікована система неефективна, то МП ефективних систем через модуль діалогу з користувачем звертається за допомогою до експерта. Використання блоків діагностики якості роботи, модуля пошуку ефективних систем, пошуку закономірностей предметної області дозволяє: підтримувати якість діагностики мережі практично без участі людини; ефективно використовувати досвід, що накопичується в процесі експлуатації.

Висновки. Отже, запропонована структура ЕС ТД ІІС дозволяє усунути недоліки в роботі ЕС з традиційною структурою. Використання концепції "вежі" обчислень у запропонованій структурі ЕС дозволяє проводити паралельне рішення завдань ТД ІІС і завдань з підвищення якості діагностики мережі. Запропонована структура ЕС ТД дозволяє рознести рішення завдань різних рівнів на дві різні ЕОМ. Такий розподіл завдань за рівнями значно спростить і прискорить роботу ЕС ТД ІІС за рахунок того, що в реальному масштабі часу вирішуватимуться тільки завдання ТД ІІС.

Список літератури

1. Постанова Кабінету Міністрів України від 17 вересня 2008 р. N 834 "Про затвердження Державної цільової науково-технічної програми створення державної інтегрованої інформаційної системи забезпечення управління рухомими об'єктами (зв'язок, навігація, спостереження)".

2. Джексон П. Введение в экспертные системы / П. Джексон. Пер. с англ. – М.: Вильямс, 2001. – 624 с.

3. Джарратано Д. Экспертные системы: принципы разработки и программирования / Д. Джарратано, Г. Райли. Пер. с англ. – М.: Вильямс, 2006 – 1152 с.

УДК 004.8

Класифікація моделей знань в експертних системах

Конопліцька-Слободенюк О.К. викладач
Кіровоградський національний технічний університет, м. Кіровоград

В сучасному світі в різних галузях життя виникає проблема з правильним отриманням знань та їх доцільного застосування. І навіть, якщо ми отримали певні знання, це ще не дає нам гарантію, що їх застосування буде корисним та раціональним і ми отримаємо бажаний результат. З цією проблемою сучасності стикається такий напрям науки, як експертні системи.

Під експертними системами можна розуміти інтелектуальні системи, здатні по ходу діалогу з людиною одержувати, накопичувати та коригувати знання з заданої предметної області, виводити нові знання, вирішувати на основі цих знань практичні задачі та пояснювати хід їх рішення.

Основна частина. Знання, доступні системі, складають базу знань цієї системи. Без бази знань систем штучного інтелекту не може існувати. Отже, знаннями інтелектуальної системи називається трійка <F, R, P>, де F - сукупність фактів, що зберігаються в пам'яті системи в явному вигляді, R - сукупність правил, які дозволяють на основі існуючих фактів отримувати нові, P - сукупність процедур, які визначають, яким чином слід застосовувати правила. Важливе місце при створенні інтелектуальних систем стає проблема представлення знань, тому виникла потреба їх класифікації. Для формалізації та представлення знань розроблені спеціальні моделі знань. На даний час моделі представлення знань класифікуються по ідеям, які лежать в їх основі та математичній обґрунтованості. Кожна з них має як переваги так і недоліки, і тому для кожної задачі необхідно використовувати таку модель, яка найбільше підходить для її вирішення, бо це буде впливати на ефективність отриманого результату.

Отже, виділяють такі моделі:

- *Продукційні моделі* – дозволяють представляти знання в вигляді таких пропозицій типу «Якщо(умова), то(дія)». Тобто, умова – це деякі пропозиції, за якими здійснюється пошук в базі знань, а дія – отримана операція при пошуку. Головні переваги таких моделей – це наочність та простота логічного виводу. Недоліками ж є те, що в базі знань накопичується багато продукційних правил і вони можуть суперечити один одному та їх зміна або додавання призводять до непередбачуваних результатів.

- *Логічні моделі* – знання представлені за допомогою логічних функцій або предикатів, що приймають значення 0 або 1 і відображають сукупність формул. Перевагами цих моделей є те, що тут присутній апарат математичної логіки, який добре вивчений. А так як логіки, що відображає мислення людини ще не існує, то це і являється недоліком даної моделі.

- *Семантичні мережі* - знання відображаються в виді графів, де вершини – це деякі поняття, а сполучення - це відношення між ними. Таке представлення дає можливість отримати структуровані знання та інформацію. Кількість типів відношень визначає сам розробник, виходячи з поставлених цілей, і вони можуть бути однорідними, якщо використовується один тип відношення, або неоднорідними, якщо кількість відношень буде більша двох. Відокремлюють мережі, які описують предметну область узагальнено та мережі, де створена конкретика з фактичних даних. Статичні бази знань в семантичних мережах можуть бути об'єктами дій, що вироблюють активні процеси з пошуку та уподібнення представленої інформації. Перевагами мережних моделей побудованих як семантичні мережі є те, що для кожної операції з знаннями або даними відокремлюється така ланка мережі, яка охоплює дані з необхідною характеристикою, представлення знань відбувається на рівні, близькому до природної мови, та можливість їх наглядно представити (графічно). Так як, мережна модель не дає чіткого представлення про структуру певної області знань, то це і є недоліком при створенні та видозмінювання таких систем.

- *Фреймові моделі* - це такі систематизовані технологічні моделі, що включають в себе пам'ять та пізнання людини. Під фреймом розуміють абстрактний образ, що представляється при отриманні деякої стереотипної інформації. Фрейм можна уявити як мережу, де є вершини і дуги, в яких нижні рівні закінчуються слотами, що заповнюються конкретною потрібною інформацією. Фрейми мають такі основні властивості:

- успадкування властивостей, тобто слот більш низького рівня вказує на слот вищого рівня, звідки неявно переносяться значення аналогічних слотів;

- базовий тип. Потрібен для того, щоб запам’ятовувати найважливішу інформацію в базовому фреймі про даний об’єкт і на її основі будувати нові фрейми для нових станів;

- процес зіставлення - процес, в ході якого перевіряється правильність вибору фрейма, здійснюється відповідно до поточної мети і інформації, що міститься в даному фреймі;

- відношення «абстрактне-конкретне» і «ціле-частка». Ієрархічна структура фреймів грунтується на відносинах «абстрактне-конкретне». На верхніх рівнях розташовані абстрактні об'єкти, на нижніх - конкретні. Об'єкти нижніх рівнів успадковують атрибути об'єктів верхніх рівнів. Ставлення «ціле-частка» стосується структурованих об'єктів і показує, що об'єкт нижнього рівня є частиною об'єкта верхнього рівня. Перевагами фреймових моделей є їх універсальність, здатність відображати концептуальну основу організації пам’яті людини, модульність. Основний недолік - відсутність механізмів управління виводу, який частково усувається за допомогою приєднаних процедур, що реалізує користувач системи.

Висновок. Для того, щоб правильно спроектувати модель знань необхідно враховувати те, що механізм керування логічними висновками та представлення знань повен бути простий в розумінні як для експертів, так і користувачів системи. Для вирішення деяких практичних задач може використовуватися декілька моделей представлення знань. Та все ж таки універсальної експертної системи не існує, бо на створення такої системи було б залучено сотні експертів з різними базами фундаментальних та здобутих інтуїтивних знань, тисячі зв’язків при їх спілкуванні, дуже потужні технічні засоби, програмні модулі, математичні обчислення, тощо.

Список літератури

1. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень: Навчальний посібник. — Запоріжжя

2. Гаскаров, Д. Б. Інтелектуальні інформаційні системи. – М.: Вищу школу, 2003

3. Ясницкий, Л. М. Введення у штучний інтелект. – М.: Академія, 2005

УДК 004.852; 004.94

Ігрова модель самоорганізації мультиагентних систем

Кравець П.О., к.т.н., доцент
Національний університет „Львівська політехніка”, м. Львів

Вступ. Самоорганізація мультиагентних систем (МАС) – це здатність колективу агентів з локальними зв’язками і цілями досягати стійких скоординованих стратегій поведінки в умовах невизначеності за рахунок самонавчання, можливості функціонувати як єдине ціле та забезпечувати виконання глобальної мети розвитку системи [1].

Враховуючи притаманні колективу агентів фактори конкуренції, взаємодії, кооперації, навчання, самоорганізації, для дослідження МАС в умовах невизначеності використаємо методи теорії стохастичних ігор, яка має спільні предмети дослідження з МАС.

Ігрова самоорганізація МАС в умовах невизначеності є актуальною науково-практичною проблемою, яка інтенсивно досліджується у сучасній науковій літературі за напрямками розподіленого штучного інтелекту та прийняття рішень.

Постановка ігрової задачі. Розглянемо множину агентів D, кожен з яких здійснює випадковий і незалежний вибір однієї із чистих стратегій $X^i = (x^i(1), x^i(2), ..., x^i(N))$ в дискретні моменти часу $n = 1, 2, ...$. На основі чистих стратегій формуються вихідні сигнали агентів $Y^i = (y^i(1), y^i(2), ..., y^i(N))$ зі значеннями у множині дійсних чисел $y^i \in R^1$. Сигнали доступні для спостереження сусіднім агентам з підмножин $D_i \subseteq D \;\; \forall i \in D \;\; (D = \underset{i \in D}{\cup} D_i)$.

Після отримання сигналів від сусідніх агентів кожен агент $i \in D$ обчислює абсолютне відхилення значень сигналів, яке відіграє роль поточного програшу гравця:

$$\xi_n^i = |D_i|^{-1} \sum_{j \in D_i} |y_n^i - y_n^j| + \mu_n^i \;\; \forall i \in D,$$

де μ_n^i – гаусівський білий шум, що імітує похибку опрацювання сигналів.

Після повторення n кроків гри середні програші агентів приймають значення:

$$\Xi_n^i = \frac{1}{n} \sum_{t=1}^{n} \xi_t^i \;\; \forall i \in D. \tag{1}$$

Метою агентів є мінімізація власних функцій середніх програшів:

$$\overline{\lim_{n \to \infty}} \Xi_n^i \to \min_{x_n^i} \;\; \forall i \in D. \tag{2}$$

Отже, на основі локального спостереження поточних програшів $\{\xi_n^i\}$ гравці повинні навчитися вибирати чисті стратегії $\{x_n^i\}$ так, щоб з ходом часу $n = 1, 2, ...$ забезпечити виконання системи критеріїв (2). У цій задачі проявом глобальної самоорганізації стохастичної гри є вирівнювання вихідних сигналів усіх гравців, що імітує поведінку популяції агентів за правилом: „діяти так як інші”.

Метод розв’язування стохастичної гри. Формування послідовності варіантів $\{x_n^i\}$ виконаємо на основі динамічних векторів змішаних стратегій $p_n^i \;\; \forall i \in D$, які приймають значення на одиничних *N*-вимірних симплексах S^N.

Гра розпочинається з ненавчених векторів змішаних стратегій зі значеннями елементів $p_0^i(j) = 1/N_i$, де $j = 1..N_i$. У наступні моменти часу динаміка векторів змішаних стратегій визначається за марківським рекурентним методом:

$$p_{n+1}^i = \pi_{\varepsilon_{n+1}}^N \left\{ p_n^i - \gamma_n \xi_n^i \left[e(x_n^i) - p_n^i \right] \right\}, \tag{3}$$

де $\pi_{\varepsilon_{n+1}}^N$ – проектор на одиничний ε-симплекс $S_{\varepsilon_{n+1}}^N \subseteq S^N$; $p_n^i \in S_{\varepsilon_n}^N$ – змішані стратегії i-го агента; $\gamma_n > 0$ та $\varepsilon_n > 0$ – монотонно спадні послідовності додатних величин; $\xi_n^i \in R^1$ – поточний програш агента; $e(x_n^i)$ – одиничний вектор-індикатор вибору варіанту $x_n^i \in X^i$.

Метод (3) отримано на основі стохастичної апроксимації умови доповняльної нежорсткості, справедливої для змішаних стратегій у точці рівноваги за Нешем [2].

У момент часу n гравець $i \in D$ на основі змішаної стратегії p_n^i здійснює випадковий вибір чистої стратегії x_n^i, за що до моменту часу $n+1$ отримує апріорі невідомий поточний програш ξ_n^i, після чого обчислює змішану стратегію p_{n+1}^i згідно з (3). Завдяки динамічній перебудові змішаних стратегій, метод (3) забезпечує адаптивний вибір чистих стратегій.

Збіжність змішаних стратегій (3) до оптимальних значень визначається співвідношеннями параметрів γ_n та ε_n, які повинні задовольняти базові умови стохастичної апроксимації [2]. Ці параметри можуть бути обчислені так:

$$\gamma_n = \gamma n^{-\alpha},\ \varepsilon_n = \varepsilon n^{-\beta},$$

де $\gamma > 0;\ \alpha > 0,\ \varepsilon > 0;\ \beta > 0$.

Ефективність самоорганізації оцінюється функціями середніх програшів (1) та середньою кількістю скоординованих стратегій гравців:

$$\mathrm{K}_n = \frac{1}{n\,|D|}\sum_{t=1}^{n}\sum_{i\in D}\chi\left(\sum_{s\in D_i}|\,y_t^i - y_t^s\,| = 0\right),$$

де $\chi(\,) \in \{0,1\}$ – індикаторна функція події.

Результати комп'ютерного моделювання. На рис. 1 у логарифмічному масштабі зображено графіки функцій середньої кількості скоординованих стратегій K_n та середніх програшів гравців Ξ_n, які характеризують ефективність самоорганізації матричної стохастичної гри. Результати отримано для значень параметрів: $|D| = 8$, $N = 5$, $\gamma = 1$, $\varepsilon = 0.999/N$, $\alpha = 0.01$, $\beta = 2$.

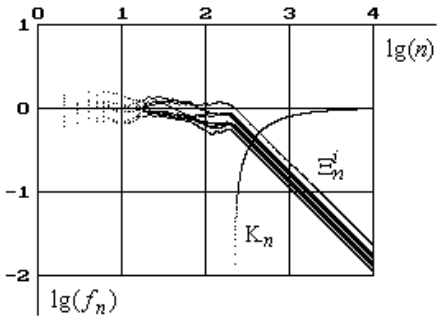


Рисунок 1 – Характеристики самоорганізації МАС

Зменшення середніх програшів Ξ_n та зростання кількості K_n скоординованих стратегій агентів свідчать про збіжність ігрового методу у силу виконання системи критеріїв (2). Зростання розмірності гри призводить до погіршення показників самоорганізації МАС.

Висновки. Запропонована ігрова модель забезпечує самоорганізацію МАС, яка виявляється у вирівнюванні стратегій гравців на глобальному рівні на основі спостереження сигналів у межах локальних підмножин гравців. Результати роботи можуть бути застосовані для забезпечення потрібної динаміки колективної поведінки МАС та у системах прийняття рішень в умовах невизначеності.

Список літератури

1. Хакен Г. Информация и самоорганизация. Макроскопический подход к сложным системам: Пер. с англ. / Г. Хакен. – М.: КомКнига, 2005. – 248 с.

2. Назин А.В. Адаптивный выбор вариантов: Рекуррентные алгоритмы / А.В. Назин, А.С. Позняк. – М.: Наука, 1986. – 288 с.

УДК 004.896

Структура экспертной системы интеллектуального регулирования микроклимата жилых помещений

Кузнецов Д.И., ст. преподаватель, к.т.н., kuznetsov-dennis@yandex.ru
Криворожский национальный университет, г. Кривой Рог

Современные системы обеспечения микроклимата жилых и производственных помещений невозможно представить без систем автоматизированного управления (САУ). Применяя САУ возможно оптимизировать работу климатического оборудования, снижая расходы на эксплуатацию, например, за счет уменьшения энергопотребления [1].

Использование современного энергосберегающего оборудования является неотъемлемым требованием при организации систем автоматического регулирования микроклимата, что, в свою очередь, позволяет обеспечить необходимый и точный уровень регулирования, например, температуры и влажности воздуха.

С точки зрения жилых помещений, таких как частные дома, квартиры или коттеджи, система микроклимата, в первую очередь, призвана организовывать комфортные условия для пребывания человека в помещении. Она должна помогать поддерживать комфортную для жильцов температуру и влажность. В свою очередь, для каждого человека существуют свои комфортные параметры климата, так как некоторые люди привыкли к прохладе, а другие - к теплу.

Целью данных исследований есть разработка структуры информационной системы интеллектуального регулирования микроклимата (ИСРМ) жилых помещений с учетом особенностей и пожеланий всех проживающих, что должно привести к упрощению процесса регулирования и автоматической подстройки под потребности каждого или группы субъектов.

Структура экспертной системы интеллектуального регулирования микроклимата жилых помещений. В общем случае процесс интеллектуального регулирования микроклимата в помещении имеет следующий вид (см. рис.1):

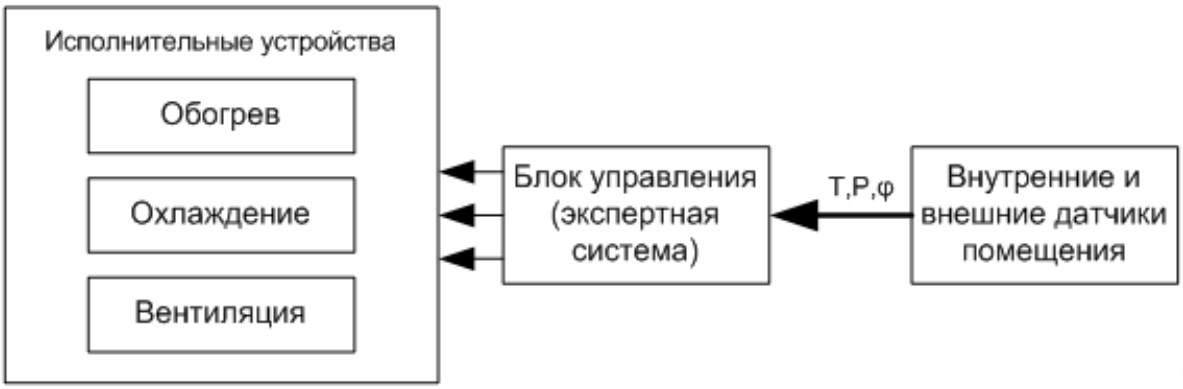


Рисунок 1 - Структурная схема процесса регулирования микроклимата

Где T - температура, P - давление, φ - относительная влажность, полученная с внутренних и внешних датчиков помещения. Блок управления являет собой экспертную систему, которая «обучается» на протяжении всей своей работы. То есть, пополняет или корректирует свою базу знаний в зависимости от изменений внутренних или внешних факторов помещения, учета дней недели или сезона года, в котором она работает. В качестве исполнительных устройств выступают радиаторы, кондиционеры и вентиляторы.

Следует отметить, что главным условием правильной и корректной работы информационной системы микроклимата является наличие соответствующих исполнительных устройств. Например, в качестве отопительных приборов следует использовать вместо привычных чугунных радиаторов, которым свойственна большая инерционность, стальные, алюминиевые или биметаллические [1].

Главным недостатком существующих информационных систем регулирования

микроклимата является отсутствие учета и подстройки под каждого субъекта помещения. На рисунке 2 представлена усовершенствованная структура экспертной системы ИСРМ с учетом пожеланий субъектов помещения.

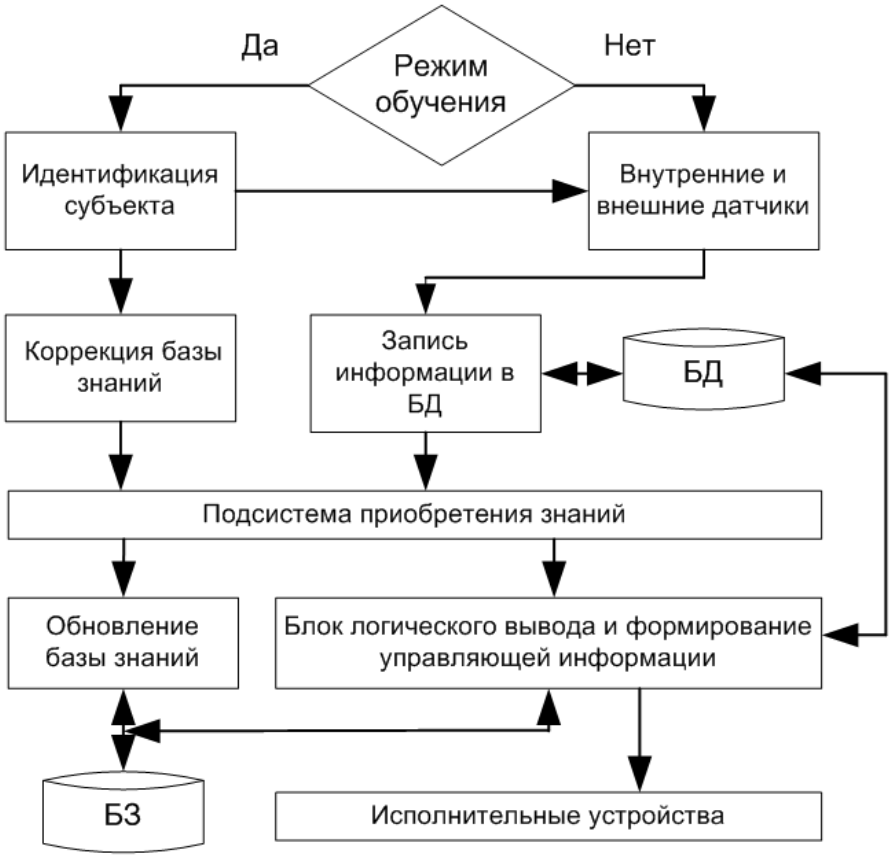


Рисунок 2 – Логико-функциональная схема работы экспертной системы

Задачей подсистемы приобретения знаний является обновление базы знаний на основе полученной информации с датчиков, а также корректированной субъектом. Следует заметить, что экспертная система (ЭС) может быть в состоянии обучения и в обычном состоянии. Цель режима обучения - получение распорядка дня, особенностей жизни субъектов помещения для дальнейшего формирования блоком логического вывода управляющей информации и достижения оптимальных условий микроклимата.

Виводы. На сегодняшний день интеллектуальные системы регулирования микроклимата являются неотъемлемой частью систем «умный дом». С учетом всех преимуществ и достижений современных методов, способов и информационных технологий регулирования микроклимата практически не существует систем, которые бы подстраивались автоматически под каждого субъекта.

Можно сделать вывод, что использование предложенной усовершенствованной ИСРМ дает возможность настроить благоприятные условия микроклимата под каждого субъекта помещения, а также уменьшить энергозатраты.

Список литературы

1. Мансуров Р. Ш. Экспериментальное исследование переходных процессов в системах обеспечения микроклимата / Сб. докладов 4-й международной научно-технической конференции «Теоретические основы теплогазоснабжения и вентиляции». – М. : МГСУ, 2011.

2. Кувшинов Ю. Я. Динамические свойства помещения с регулируемой температурой воздуха // Известия вузов. Строительство и архитектура. – 1993. – № 4

УДК 004.891

Проектування гри «Точки»

Кущевський Д.Р., учень 10-го класу, учень Малої академії наук учнівської молоді,
dima.kushhevskij@mail.ru
Науковий керівник – Дрєєв О.М., к.т.н., викладач
Кіровоградський обласний навчально-виховного комплексу
(гімназія – інтернат – школа мистецтв), м. Кіровоград

В роботі розглянуто процес створення програми для проведення логічної гри “Точки” проти комп’ютерного алгоритму. Аналіз програм, які реалізують гру, показав відсутність реалізацій штучного інтелекту, який би міг перемогти середнього гравця-аматора. Також, проаналізовані програми мають суттєві недоліки що до автоматизації процесу обведення точок супротивника. Тому створення нових алгоритмів оцінювання ігрової ситуації “Точки” та вдосконалення алгоритмів обведення точок супротивника є актуальною задачею не лише в реалізації гри, але й для винайдення нових шляхів розвитку методів алгоритмічного прийняття рішень.

Запропоновано метод пошуку контурів методом обходу “правої руки”, де можливість обведення додатково перевіряється за наявністю в знайденому контурі точок супротивника. Також, для оцінювання ігрової ситуації створено повну базу можливих ситуацій на ділянці поля 3x3.

Опис алгоритму пошуку контуру. Ігрове поле представлено в програмі у вигляді двовимірної таблиці, де точки одного кольору позначені певним числом. З причини, що новий контур може утворитися лише щойно встановленою точкою, контур шукається рекурсивним алгоритмом за правилом правої руки, саме від цієї точки. В ситуації повернення до початкової точки, отримуємо факт наявності контуру. По завершенню рекурсивного виклику на початковій точці, контур позначається окремим числом. В результаті перевірки за доступними напрямками, матимемо позначення всіх можливих обведень.

Опис алгоритму можливості обведення. Наявність контуру дає можливість обведення лише при наявності ворожих точок в усередненні цього контуру. Тому, на додатковій таблиці проводиться зовнішня “заливка” поля, як частини растрового малюнка. З причини великої кількості точок, рекурсивний алгоритм фарбування не є застосовний, тому використано більш повільний, але не рекурсивний алгоритм фарбування. Можливість процедури обведення підтверджується наявністю на незафарбованій ділянці ворожої точки. Хід в заздалегідь обведену зону опрацьовується окремо.

Опис алгоритму визначення відповіді на хід людини. Для прийняття рішення про виконання ходу-відповіді, створено повний перелік ігрових ситуацій 3x3, що складає 3^9 варіантів. Кожна комбінація має свій порядковий номер, який отримується за допомогою запису комбінації у вигляді трійкового числа з 9-ти знаків. Кожна комбінація супроводжується байтовою оцінкою важливості комбінації, кожен варіант ходу-відповіді теж має байтову оцінку. На початку роботи програми всі оцінки є однаковими і рівні 127, лише комбінації, де хід не можна зробити, завчасно позначені важливістю 0. Також для всіх зайнятих позицій в обраній комбінації, хід-відповідь теж має значення 0. Відповідні комбінації початкового стану згенеровані окремою програмою.

Система в процесі гри змінює значення оцінок в додатню сторону, при факті обведення та в від’ємну сторону — при обведені точок супротивником. Якщо аналіз ситуації показує рівноправні варіанти, то ход-відповідь обирається випадково з знайдених рівнозначних ходів. Завдяки корегуванню значень коефіцієнтів значності ситуації та значності ходу, програма набуває досвіду і з часом її гра стає сильнішою. В майбутньому планується реалізувати алгоритм гри програми із собою для збільшення кількості партій для набуття досвіду.

На жаль, збільшення поля до 4x4 призводить до збільшення кількості можливих варіантів 3^{16}. Таку кількість варіантів в повній таблиці зберігати не можливо. Тому для застосування розробленого метода пошуку ходу-відповіді потрібно розробити систему евристики відкидання значного відсотку програшних ходів.

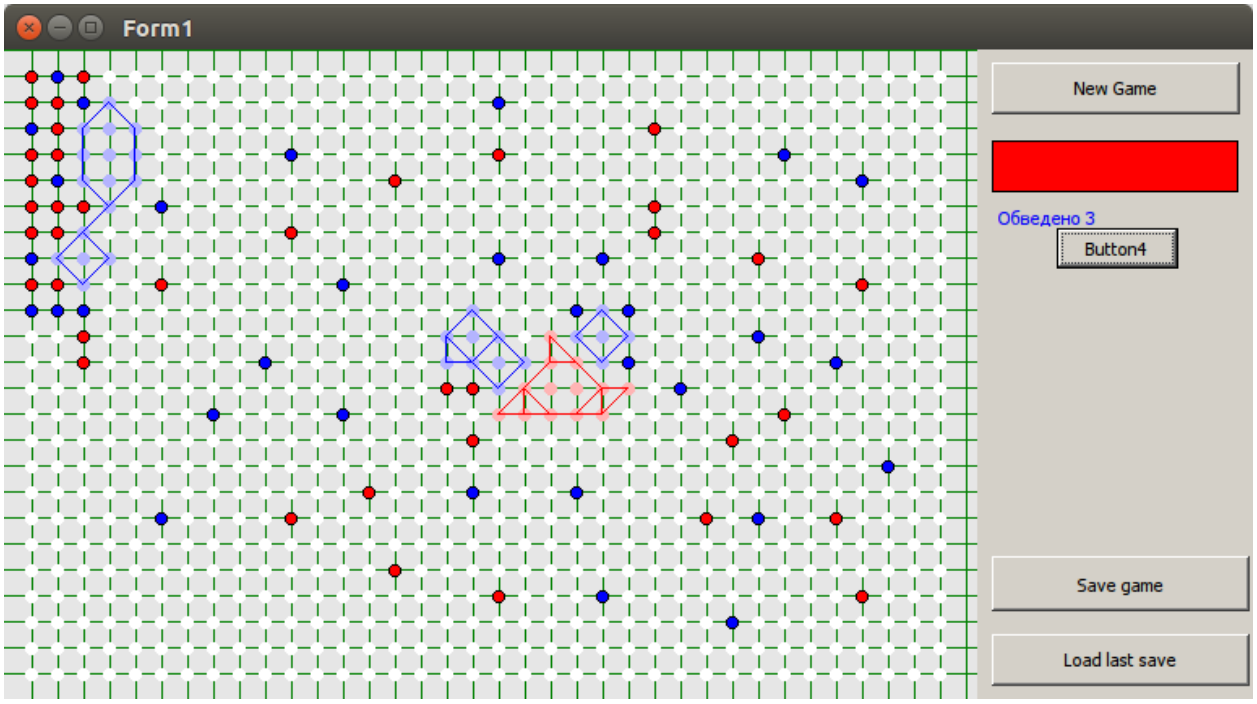


Рисунок 1 — Зовнішній вигляд програми для гри в "Точки"

Висновки. Розроблені алгоритми реалізації гри "Точки" є готовим продуктом, який якісно виконує правила обведення ворожих точок. Штучний інтелект є слабким, хоча має здатність до самонавчання. Отримані алгоритми та принципи є придатними до подальшого вдосконалення.

Список літератури

1. Алексеев Е.Р., Чеснокова О.В., Кучер Т.В. Самоучитель по программированию на Free Pascal и Lazarus. - Донецк.: ДонНТУ, Технопарк ДонНТУ УНИТЕХ, 2011. - 503 с.

2. Кетков, Ю.Л. Свободное программное обеспечение. FREE PASCAL для студентов и школьников / Ю. Л. Кетков, А. Ю. Кетков. — СПб.: БХВ-Петербург, 2011. — 384 с.

3. Мансуров К.Т. Основы программирования в среде Lazarus, 2010. – 772 с.

4. Ахо, Альфред, В., Хопкрофт, Джон, Ульман, Джеффри Структуры данных и алгоритмы. : Пер. с англ. : М. : Издательскийдом "Вильяме", 2003. — 384 с.

5. Бакнелл Джулиан М. Фундаментальные алгоритмы и структуры данных в Delphi: Пер. с англ./Джудиан М. Бакнелл. - СПб: ООО "ДиаСофтЮП", 2003. - 560 с.

УДК 004.89:004.822

Використання автоматично побудованих синтаксичних шаблонів для виявлення та обробки семантичних зв'язків у тексті

Левошко О.Л., старший викладач кафедри програмування та захисту інформації,
Levoshkoel@ukr.net
Кіровоградський національний технічний університет, м. Кіровоград

Дана робота присвячена дослідженню й розробці методів автоматичного виявлення та обробки семантичних відношень в тексті. Під обробкою семантичного зв'язку мається на увазі визначення в тексті пар імен сутностей, що перебувають в даному відношенні (зв'язку). Приклади семантичних відношень - «працювати_на» (ім'я людини і його місце роботи), «створена_в» (назва організації та дата її створення). Завдання обробки семантичних відношень належить до галузі інтелектуального аналізу текстів, вкрай актуальної та затребуваної в даний час. Алгоритми обробки семантичних відношень можуть застосовуватися для покращення методів пошуку ключових слів у текстах, для автоматичного створення баз даних, а також для розширення інтерфейсу пошукових систем.

Для вирішення завдання обробки семантичних відношень з текстів був використаний метод, заснований на автоматичному створенні синтаксичних шаблонів, що є релевантними для шуканих відношень. Метод побудовано на алгоритмі активності, котрий розповсюджується на семантичній мережі. Запропонований метод складається з двох етапів:

1. На першому етапі автоматично будується набір синтаксичних шаблонів. Кожен шаблон моделюється піддеревом дерева синтаксичного розбору речень. Для побудови шаблонів використовується текстовий файл і набір пар імен сутностей, які перебувають у початковому відношенні. Також на даному етапі обчислюються оцінки, що характеризують якість шаблонів.

2. На другому етапі побудовані раніше синтаксичні шаблони застосовуються до речень цільового тексту. При цьому формуються пари імен сутностей, що претендують на наявність шуканого семантичного відношення між ними. Рішення про включення кожної пари імен до результуючої множини приймається на підставі оцінок застосованого шаблону, за допомогою якого була вибрана дана пара імен, семантичної близькості слів речення, з якого була вибрана пара імен, до набору ключових для даного відношення слів, точності відповідності речення до шаблону.

Висновок. Запропонований метод обробки семантичних відношень в тексті показав досить високу точність (70%) на тестових даних для відношення «працювати_на».

Список літератури

1. [Електронний ресурс]. – Режим доступу: http://www.dictum.ru. Матеріали з автоматичної обробки текстів.

2. [Електронний ресурс]. – Режим доступу: http://www.aot.ru. Матеріали з автоматичної обробки текстів.

3. Lei Shi. An Algorithm for Open Text Semantic Parsing / Lei Shi, Rada Mihalcea // Proceedings of the ROMAND 2004 Workshop on «Robust Methods in Analysis of Natural Language Data». – 2004.

НАУКОВЕ ВИДАННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

“ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ”

INFOSEC & COMPTECH

24-25 березня 2016 року

Тези доповідей надруковано в авторській редакції.

Відповідальна за випуск: Мелешко Є.В.

Підписано до друку 18.03.2016
Тираж 60 прим.

©Кафедра програмування та захисту інформації КНТУ,
м.Кіровоград, пр.Університетський, 8.
Тел. (0522) 39-04-49
