Управління розвитком

Харківський національний економічний університет

І міжнародна науково-практична конференція "Безпека та захист інформації в інформаційних і телекомунікаційних системах"

Секція 1
"Методи та технології безпеки інформаційних систем"

Секція 2
"Захист інформації в комп'ютерних системах"

Секція 3
"Інформаційні та телекомунікаційні системи в бізнесі"

28 – 29 травня 2008 року

Збірник наукових статей

видається 2 рази на рік

№ 7, 2008

Харків. Вид. ХНЕУ, 2008

ЗБІРНИК НАУКОВИХ СТАТЕЙ

Управління **РОЗВИТКОМ** №7'2008

Засновник і видавець

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Реєстраційний номер свідоцтва КВ №5948 від 19 березня 2002 р.
Затверджено на засіданні вченої ради університету.
Протокол №9 від 21.04.2008 р.

Адреса видавця: *61001, Україна, м. Харків, пр. Леніна, 9а*
Телефони:
(057)702-03-04 — головний редактор
(057)758-77-05 — зав. редакції
E-mail: *vydav@ksue.edu.ua*

Підписано до друку 19.05.2008 р.
Формат 84×108 1/16. Папір MultiCopy.
Ум.-друк. арк. 12,0. Обл.-вид. арк. 15,12. Тираж 500 прим. Зам. № 409.
Ціна договірна.

Надруковано з оригінал-макета на Riso-6300 61001, м. Харків, пр. Леніна, 9а.
Видавництво ХНЕУ.

Секція 1
Методи та технології безпеки інформаційних систем

УДК 004.78:336.717

Бутова Р. К.

Гаврилова А. А.

ТЕХНОЛОГІЯ АУТЕНТИФІКАЦІЇ ЯК ЗАСІБ БЕЗПЕКИ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сьогодні неможливо уявити функціонування банківських установ без використання сучасних інформаційних технологій та, зокрема, глобальних комп'ютерних мереж, у тому числі й Internet. Це пояснюється тим, що онлайнові банківські послуги дозволяють проводити фінансові операції (торгівля акціями, отримання кредитів, страхування і т. п.) без посередників, що призводить до зниження комісійних і прискорення обігу фінансових активів.

Актуальність даної теми пов'язана з відстеженням розвитку та сучасного становища ринку банківських Internet-послуг і важливістю безпеки проведення Internet-платежів.

На користь використання сучасних інформаційних технологій для проведення банківських операцій, що здійснюються як з юридичними, так і з фізичними особами, свідчить дослідження, проведене консультаційною фірмою Booz, Allen and Hamilton. За його результатами оплата послуг через Internet обходиться клієнту в $ 0,01, з використанням автоматів – у $ 0,27, надання послуг по телефону – $ 0,54, а в касового вікні – у $ 1,07 [1].

Фінансові інститути прагнуть знизити величезні витрати з утримання своїх філій і відділень, а також витрати з обов'язкових платіжних перерахувань, одночасно вони намагаються підвищити і прибуток окремих кредитних установ. Обсяг послуг банку, які надаються за допомогою Internet, постійно зростає. Так, ще на початку XXI століття тільки 5 % фінансових установ України надавали доступ через Internet, а на початку 2008 року їх кількість становить 65 %. Для порівняння: у Європі 70 % банків надають послуги в он-лайн режимі. За оцінками компанії Garther обсяги комерційних трансакцій у Європі зростуть за найближчі чотири роки з $ 65 млрд. до $ 2 200 млрд. [2]. Величезне розмаїття електронних банківських продуктів і послуг стосується, в першу чергу, такої важливої сфери, як національний і міжнародний платіжний оборот. Система електронних розрахунків зводить до мінімуму банківські операції (розрахунки, платіжні доручення, інформаційне забезпечення) з обслуговування клієнтів у касах. Поряд з цим все ширше використовуються банкомати, за допомогою яких клієнтам видається не лише готівка, але й можливість покласти кошти на рахунок, зробити операції за ощадною книжкою клієнта і т. д., тобто система розрахунків готівкою замінюється системою безготівкових розрахунків і платежів.

У даний час мережа Internet уже є інформаційною системою для оперативного здійснення банківських операцій. Разом з тим відкритість цієї мережі для платежів і використання її як каналу збуту викликає у користувачів різного роду сумніви щодо безпеки. Щоденно у світі $ 2000 млрд. перераховуються з використанням електронних систем зв'язку. За даними Бюро технологічної оцінки США 0,05 – 0,1% усіх переказів відносяться до відмивання "брудних" коштів. Річні збитки від шахрайських дій з пластиковими картками складають менше половини одного відсотка від загального грошового обігу – приблизно $ 1,3 мільярда. Хоча збитки становлять і невеликий відсоток від загального обсягу, але сама сума є вражаючою. Постійне збільшення цієї цифри свідчить про існування кримінальної підпільної індустрії, пов'язаної з незаконним використанням пластикових карток. У дослідженні, опублікованому американською фірмою ClearCommerce, Україна називається вогнищем кібершахрайства – тут відбувається більшість шахрайських операцій із кредитними картками. Висновки дослідження свідчать, що 20% усіх замовлень, які надходять з України, є шахрайськими – "замовники" використовують украдену інформацію з кредитних карток [3].

Отже, одночасно з розширенням мережі користувачів банківських установ і спрощенням процедури доступу до них збільшується кількість загроз як до комп'ютерних систем, так і до фінансової організації у цілому. Поширення так званої комп'ютерної злочинності у банківсько-кредитній сфері пояснюється дуже просто – адже саме у даній сфері знаходяться величезні фінансові кошти, які в першу чергу цікавлять злочинців. Тому значну роль відіграє розробка таких технологій безпеки, застосування яких призвело б до зменшення цих загроз.

Для зменшення випадків шахрайства в Internet платіжні системи запропонували банкам і торговим підприємствам при проведенні розрахунків платіжними картами використовувати технологію 3-D Secure [4]. Такі платіжні системи, як Visa Internetional та MasterCard Worldwide активно просувають цю технологію у всьому світі, висовуючи вимогу застосовувати її всім банкам та підпри-

ємствам, які бажають з ними співпрацювати. Суть цієї технології полягає в тому, що вона забезпечує безпечність проведення розрахунків у мережі Internet, зменшуючи ризики з шахрайства банка-еквайєра, який на свій ризик раніше сам проводив чи не проводив платіж емітента. З прийняттям платіжними системами даної технології, емітент позбувається можливості відмовитись від платежу з причини невизнання операції утримувача карти.

В основі цієї технології лежить однойменний протокол, який було розроблено міжнародними платіжними системами з метою підвищення безпеки платежів, що проводяться через Internet, та в мобільній комерції. Технологія 3-D Secure відноситься до класу технологій аутентифікації клієнта, яка використовує протокол SSL (Secure Stockets Layer) для захисту даних, що передаються відкритими каналами, та модуль Merchant Plug-in (MPI). Цей модуль забезпечує передачу даних між постачальником послуг та учасниками системи та захист конфіденційних даних утримувача карти.

Протокол використовує у мережі Internet структуру трьох доменів − емітента, еквайєра та загального. Домен емітента використовується для обслуговування запитів утримувача карти до сервісу аутентифікації та включає в себе ідентифікацію користувача при звертанні до сервісу та аутентифікацію у процесі проведення платежу. Аутентифікація може бути проведена кількома способами, наприклад, шляхом введення секретного коду, використання смарт-карти для формування криптограми. Домен еквайєра використовується для обслуговування торгівельних точок, що забезпечує процедури для їх функціонування згідно зі стандартними протоколами та виконання процесингу транзакцій, які пройшли аутентифікацію. Загальний домен забезпечує взаємодію доменів емітента та еквайєра шляхом надання засобів передачі даних запитів і загальних протоколів взаємодії, що гарантує взаємну аутентифікацію один одного. Таким чином, можна говорити про існування так званої моделі трьох доменів, яка розбиває процес на окремі зони. В зоні домена емітента знаходиться утримувач карти, а в зоні домена еквайєра − торгівельне підприємство. Взаємодія між ними забезпечується через загальний домен.

Порядок проведення платежів з використанням 3-D Secure починається з реєстрації клієнта. Реєстрація виконується до початку проведення платежів у мережі Internet. Процес реєстрації проводиться на сервері емітента, де у клієнта запитується інформація про дані його карти та секретні коди. Як секретний код може бути використано запитання з заздалегідь відомою клієнту та емітенту відповіддю. Дана технологія є найбезпечнішою, а це впливає на конкурентоспроможність магазинів та лояльність утримувачів карти. При проведенні покупки за допомогою 3-D Secure утримувач карти отримує нові переваги, які гарантують йому захист від шахрайства.

Переваги використання даної технології при проведенні платежів через Internet надаються кожному суб'єкту платіжної системи. Так, Internet-магазин підвищує свою привабливість для покупців, шляхом забезпечення рівня безпеки проведення їх платежів. Також він знижує свої прямі витрати, пов'язані з поверненням коштів клієнтам і тимчасові адміністративні витрати з опрацювання претензій клієнтів, бо при застосуванні даної технології при проведенні платежу по карті, його не можна заперечувати, оскільки він вважається однозначно ідентифікованим на правомірність та легітимність. Для банків ця система дозволяє знижувати витрати на утримування філій і персоналу та отримувати прибутки, пов'язані з нарахуванням відсотків за користування їх коштами. Загалом використання технології 3-D Secure повинно підвищити довіру з боку покупців, продавців та утримувачів карт до проведення платежів у мережі Internet, і як наслідок − прискорити розвиток ринку електронної комерції в цілому та знизити ризики в сфері шахрайства при проведенні електронних платежів.

Література: 1. http://www.liga.kiev.ua/news/show 2. http://www.softlab.ru/products/inbank/nfsec.asp 3. Концепция безопасности коммерческого банка // Бизнес и безопасность. – 2007. – №4 (60). – С. 51 – 57. 4. Куделя Е. Безопасность Интернет-платежей / Е. Куделя, Н. Реном // Карт-Бланш. – 2007. – №21. – С. 16 – 18.

Андрущенко Д. М.

Козина Г. Л.

УДК 004.056

АНАЛИЗ СТОЙКОСТИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ К КОМПРЕССИИ ИЗОБРАЖЕНИЙ

В настоящее время обострилась проблема защиты авторских прав на цифровую информацию, в том числе и на цифровые изображения. Одним из способов ее решения является внедрение скрытой информации в оригинал изображения − цифрового водяного знака (ЦВЗ). При этом предъявляется два обязательных условия:

отличие изображения со встроенным ЦВЗ от оригинала должно быть незаметно человеческому глазу;

встроенный ЦВЗ должен быть устойчивым (робастным) к различным методам обработки изображения.

Известно много методов встраивания ЦВЗ [1; 2], однако среди них нет таких, которые бы удовлетворяли стойкостью ко всем методам обработки изображения. Поэтому в каждом конкретном случае необходимо выбирать определенный метод встраивания ЦВЗ, или объединять несколько методов одновременно. Робастные алгоритмы встраивания ЦВЗ, в основном, основаны на изменении коэффициентов в частотной области преобразования изображения. Такие алгоритмы обычно допускают изменение некоторых параметров (или параметра), влияющего на степень робастности ЦВЗ. Однако чем больше стойкость, тем более отличается изображение со встроенным водяным знаком от исходного. Поэтому величины параметров алгоритмов всегда выбираются из соображения компромисса между величиной искажения оригинала изображения и робастностью ЦВЗ. Некоторые авторы предлагают использовать пороговое значение JND [2; 3], которое вычисляется из условия достижения максимального искажения изображения невидимого человеческим глазом. Однако зрительная система индивидуальна для каждого человека, кроме того, в некоторых случаях могут быть предъявлены другие условия к величине допустимого искажения оригинала.

В данной работе предлагается производить выбор параметров алгоритма, исходя из условий, предъявляемых к стойкости. Для этого необходимо экспериментальным путем проверить стойкость ЦВЗ встроенных в одни и те же изображения при различных параметрах алгоритма.

Приведенный подход был исследован путем оценки стойкости ЦВЗ встроенных по первому варианту алгоритма Коха и Жао [1] к JPEG-компрессии изображений. Для этого было отобрано 10 фотографий размером 200x150 пикселей. В канал синего цвета каждой из них был внедрен ЦВЗ, представляющий собой битовое изображение размером 20x15 пикселей. Исследуемый параметр − значение порога встраивания изменялось от 5 до 55 с шагом 5. Каждое из 110 полученных изображений было подвергнуто компрессии с различными коэффициентами, изменяющимися от 11 до 2 с шагом 1. Из всех сжатых изображений (1100 шт.) извлекался ЦВЗ и сравнивался с оригиналом. Величина совпадения определялась по формуле:

$$\rho = \frac{\sum_{i=1}^{N} w_i \widehat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2} \sqrt{\sum_{i=1}^{N} \widehat{w}_i^2}},$$

где $w_i, \widehat{w}_i$ − элементы оригинального и извлеченного водяного знака;

N − количество бит водяного знака.

По результатам исследований сделан вывод, что метод Коха и Жао может быть использован только в том случае, если не требуется стойкость к компрессии с коэффициентом меньшим 6. Некоторые изображения, в которых преобладает синий цвет, визуально отличаются от оригинала при встраивании ЦВЗ со значением порога встраивания большим 35. Для таких изображений стойкость к разрушению ЦВЗ обеспечивается только при сжатии с коэффициентом не менее 7. В такие изображения лучше встраивать ЦВЗ в канал красного либо зеленого цвета.

Література: 1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко.– К.: "МК-Пресс", 2006. – 288 с. 2. Chen L.-H. Mean quantization based image watermarking. / L.-H. Chen, J.-J. Lin // Image and Vision Computing. – Vol. 21 – №8. – 1 August 2003. – P. 717 – 727. 3. Eyadat M. Performance evaluation of an incorporated DCT Block-Based Watermarking algorithm with Human Visual system Model / M. Eyadat S. Vasikarla,, Pattern Recognition Journal.– Vol. 26. – 2005. – pp. 1405 – 1411.

УДК 681.3

Смірнов О. А.

Доренський О. П.

ВИЗНАЧЕННЯ ВАГОВИХ КОЕФІЦІЄНТІВ КЛАСІВ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА ЇХ ЗАСТОСУВАННЯ

На сьогоднішній день існує безліч методів визначення коефіцієнта відносної важливості вимог до параметрів систем забезпечення безпеки інформації (СЗБІ). Дослідження [1] дає підстави зробити висновок про складність їх реалізації та практичного застосування. Зокрема, методи, дос-

ліджені в джерелі [2], потребують якісної вхідної експертної інформації про параметри системи, яка досліджується або проектується. Це, у свою чергу, породжує проблеми й труднощі, які можуть призвести до великих похибок результуючих характеристичних величин [3].

Крім того, застосування більшості методів оцінювання вагових коефіцієнтів вимагає визначення ступенів взаємозв'язків та взаємовідношень між параметрами СЗБІ (наприклад, їх залежності чи незалежності один від одного), виходячи з чого експерт приймає рішення про застосування відповідного методу. На нього також мають великий вплив складність і трудоємкість експертизи, що визначається реальними умовами та можливістю проведення.

Було проведено детальний аналіз загроз інформації інформаційної системи (ІС), їх властивостей і характеристик [4]. Також обґрунтовано необхідність окремого врахування загроз, атака яких направлена безпосередньо на СЗБІ, яка, по суті, й визначає рівень безпеки інформації ІС. Класифікацію загроз ІС здійснено на чотири класи: I – апаратні (техногенні), II – програмні, III – природні (стихійні), IV – людські (антропогенні). При цьому клас IV поділено на два підкласи: IV.I – суб'єктивні (навмисні) та IV.II – об'єктивні (ненавмисні) загрози. В результаті одержано вагові характеристики кожного з чотирьох класів загроз, які характеризують величину завданого збитку ІС загрозою відповідного класу α: $\alpha_1 = 0.11$, $\alpha_1 = 0.11$, $\alpha_1 = 0.13$, $\alpha_1 = 0.65$ ($\sum_i \alpha_i = 1$) [4]. Прийнявши одержану величину α за показник, який характеризує рівень необхідності протидії загрозі даного класу, отримуємо досить ефективний і, в той же час, надзвичайно простий у практичному застосуванні метод визначення вагових характеристик параметра СЗБІ, який забезпечує протидію даній загрозі. Величину α назвемо коефіцієнтом класу загроз (ККЗ) безпеці інформації ІС.

Таким чином, для визначення вагової характеристики параметра СЗБІ необхідно ідентифікувати загрози, яким він протидіє, та присвоїти ККЗ α значення ваги відповідного класу загроз ІС, тобто $\alpha = \alpha_i$ при $1 \le i \le 4$, $0 < \alpha < 1$. Якщо він забезпечує захист відразу від загроз декількох класів, то його вага визначається сумою коефіцієнтів α_i відповідних класів. Як показали дослідження [1; 3], більшість систем оцінювання показника якості СЗБІ реалізовані програмно. З цього випливає, що і методи, застосовані для реалізації системи, повинні бути максимально простими й зручними для представлення і введення експертом вхідних експертних даних і виведення йому вихідних даних. Запропонований метод визначення ККЗ відповідає цим вимогам, що є свідченням його ефективності та практичної цінності.

Розглянуто алгоритм практичної реалізації запропонованого методу, розроблено програмний модуль застосування ККЗ та його практичне застосування в системі оцінювання якості СЗБІ ІС. Крім того, наводяться нові результати аналізу класифікації [4], зокрема виявлені числові та функціональні залежності між класами загроз безпеці інформації ІС. Пропонуються можливі напрямки подальшого дослідження й застосування.

Література: 1. Доренський О. П. Метод визначення коефіцієнтів відносної важливості вимог до параметрів системи забезпечення безпеки інформації // Захист інформації. – №4(36). – К.: ДУІКТ, 2007. – С. 45 – 52. 2. Анохин А. М. Методы определения коэффициентов важности критериев / А. М. Анохин, В. А. Глотов, В. В. Павельев, А. М. Черкашин // Автоматика и телемеханика. – 1997. – №8. – С.3 – 36. 3. Доренський О. П. До питання визначення часткових показників матриці оцінок та коефіцієнтів відносної важливості вимог до параметрів системи забезпечення безпеки інформації / О. П. Доренський, С. Б. Воропай // Системи обробки інформації. – 2007. – Вип. 8 (66). – С. 95 – 99. 4. Доренський О. П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу // Зб. наук. пр. Кіровоградського національного технічного університету.– 2007. – Вип. 19. – С. 55 – 61.

Єсаулов М. Ю.

УДК 621.391.7

СТРУКТУРА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ПРОЦЕСУ УПРАВЛІННЯ ЗАХИСТОМ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Ефективне забезпечення захисту в інформаційних системах (ІС) можливе тільки на основі комплексного використання усіх відомих методів і підходів до вирішення даного завдання. Концепція такого комплексного захисту повинна задовольняти наступну сукупність вимог. По-перше, мають бути розроблені й доведені до рівня регулярного використання всі необхідні механізми гарантованого забезпечення необхідного рівня захищеності інформації. По-друге, повинні існувати механізми

практичної реалізації необхідного рівня захищеності інформації. По-третє, необхідно мати у своєму розпорядженні засоби раціональної реалізації всіх необхідних заходів щодо захисту інформації на базі досягнутого рівня розвитку науки й техніки. І, нарешті, по-четверте, мають бути розроблені способи оптимальної організації й забезпечення проведення всіх заходів щодо захисту в процесі обробки інформації.

На основі аналізу розвитку концепції захисту інформації неважко зробити висновок про те, що має місце тенденція постійного зростання зусиль, які вкладаються у захист, вдосконалення підходів до захисту й самих механізмів захисту. Проте слід зазначити й той факт, що традиційна архітектура ІС і технологія автоматизованої обробки інформації не забезпечує всіх умов, необхідних для надійного захисту інформації.

Одним із основних підходів до проблеми захисту інформації є положення про те, що в сучасних і перспективних ІС ефективний захист інформації не може бути забезпечений простим включенням до складу системи деяких механізмів і пристроїв захисту − захистом інформації необхідно постійно управляти.

Управління захистом інформації [1] становить складну сукупність взаємопов'язаних процесів безперервного створення, вдосконалення й контролю над системою механізмів захисту, які використовуються в ІС. При цьому важливою є та обставина, що підсистема управління захистом інформації є сукупністю однорідних у функціональному відношенні заходів, регулярно здійснюваних в ІС з метою створення, підтримки й забезпечення умов, об'єктивно необхідних для забезпечення надійного захисту інформації необхідного рівня.

Враховуючи той факт, що управління захистом інформації є окремим випадком управління в системах організаційно-технологічного типу, процес проектування систем захисту інформації спрощується, оскільки для цього досить трансформувати загальні положення концепції управління в системах вказаного типу на проблеми управління захистом інформації.

Надійний захист інформації в ІС може бути ефективним лише в тому випадку, якщо він буде виконуватися для всіх елементів системи [2], що потребують захисту, з боку множини потенційно можливих загроз, при постійному контролі показників рівня захищеності системи.

Для визначення рівня захищеності повинен здійснюватися відповідний контроль, на основі якого визначиться показник рівня захищеності. Основними характеристиками контролю є: повнота контролю, кількість охоплюваних контролем елементів системи, час і періодичність проведення контролю, послідовність контрольних операцій, які проводяться, режим проведення контролю, ступінь автоматизації контрольних операцій, аналіз і оцінка ходу виконання контролю механізмів захисту з метою своєчасного й правильного ухвалення рішення.

Аналіз відомих методик оцінки захищеності систем [3; 4] інформаційних технологій дає можливість зробити висновок, що велика група методик оцінки базується на наявності певного набору засобів й механізмів захисту, методик виготовлення експлуатації й тестування та дозволяють віднести той або інший пристрій або систему інформаційних технологій до одного з дискретних рівнів захищеності відповідно до використовуваних в даній країні стандартів.

Огляд публікацій за даною тематикою показав, що оцінки відображають статичний стан об'єкта захисту, виходячи з наявних механізмів захисту, не враховують дійсну завантаженість цих механізмів захисту щодо нейтралізації наслідку загроз, динаміку зміни множини загроз, можливість адаптації системи захисту інформації до зміни множини загроз, не дають вказівок на зміну складу механізмів захисту та структури багаторівневої системи інформаційної безпеки (СІБ).

Розвиток інформаційно-телекомунікаційних систем відбувається у напрямі створення інтелектуальних засобів з елементами самоорганізації, в яких присутні процеси зародження, адаптації та розвитку.

Таким чином, у доповіді розглядається структура системи підтримки прийняття рішення процесу управління захистом інформації в ІС, що базується на адаптивній моделі системи інформаційної безпеки. Це дозволяє реалізацію наступної послідовності заходів: оцінку фактичного стану інформаційної безпеки ІС, прогнозування стану інформаційної безпеки системи й ступеня впливу загроз і дестабілізуючих чинників, планування системи заходів захисту інформації відповідно до факторів загроз і поточного значення захищеності системи, визначення методів і механізмів забезпечення необхідного рівня захищеності та прийняття рішення щодо управління системою захисту інформації.

Література: 1. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Изд. Наука и техника, 2004. – 384 с. 2. Вертузаєв М. С. Захист інформації в компютерних системах від несанкціонованого доступу. Навч. посібник / М. С. Вертузаев, О. М. Юрченко; [За ред. С. Г. Лаптєва. – К.: ЄУФІМБ, 2001. – 321 с. 3. Партыка Т. Л. Информационная безопасность. Учебное пособие / Т. Л. Партыка, И. И. Попов. – М.: ФОРУМ: ИНФРА-М, 2002. – 368 с. 4. Габарчук В. Кибернетический подход к проектированию систем защиты информации / В. Габарчук, З. Зинович, А. Свиц. – К.: Киев-Луцк-Любляны, 2003. – 653 с. 5. Петров В. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с. 6. Нестерук Г. Ф. Адаптивная модель нейросетевых систем информационной безопасности / Г. Ф. Нестерук, Л. Г. Осовецкий, Ф. Г. Нестерук // Перспективные информационные технологии и интеллектуальные систем. – №3 (15). – 2003.– С. 14 – 16. 7. Герасимов Б. М. Системы поддержки принятия решений: проектирование, применение, оценка эффективности / Б. М. Герасимов, М. М. Дивизюк, И. Ю. Субач. – Севастополь: Научно-исследовательский центр вооруженных сил Украины "Государственный океанариум", 2004. – 320 с.

Кобозева А. А.

УДК 004.056.5:518

АНАЛИЗ СВОЙСТВ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ И ПРОЦЕССОВ НА ОСНОВЕ ТЕОРИИ ВОЗМУЩЕНИЙ

Проблема информационной безопасности для современного общества, решение которой неотделимо от анализа состояния информационных объектов (ИО), является чрезвычайно значимой и актуальной [1]. Однако до настоящего времени оставался нерешенным вопрос создания единого математического подхода к такому анализу, что является целью данной работы. Предлагается новый единый математический подход к оценке состояния произвольных ИО, основанный на теории возмущений [2].

Для достижения поставленной цели необходимо решить следующие задачи: разработать общие формальные модели произвольных непрерывного и дискретного информационных процессов (ИП); на основании разработанных моделей выделить набор параметров, анализ возмущений которых определяет характеристики исследуемых процессов (объектов).

Любой ИП в самом общем виде можно представить как некоторую непрерывную вектор-функцию конечного числа переменных:

$$\Phi(x_1,..., x_n) = \begin{pmatrix} \varphi_1(x_1,..., x_n) \\ \varphi_2(x_1,..., x_n) \\ \vdots \\ \varphi_m(x_1,..., x_n) \end{pmatrix} = \begin{pmatrix} \Phi_1 \\ \Phi_2 \\ \vdots \\ \Phi_m \end{pmatrix}, \quad (1)$$

где $(\Phi_1, \Phi_2,..., \Phi_m) \in R^m$ – выходные, а $(x_1,..., x_n) \in D(\Phi) \subseteq R^n$ – входные параметры, несущие в себе всю ценную информацию об основных закономерностях процесса. Функция (1) порождает на $D(\Phi)$ m функций:

$$\varphi_i(x_1,..., x_n) = \Phi_i, \ i = \overline{1,m}. \quad (2)$$

Утверждение 1. Произвольный непрерывный ИП (или ИО, рассматриваемый как результат процесса его синтеза) может быть формально представлен в виде конечного множества функций (2), а анализ этого процесса сведен к анализу полученных функций.

Построение функции (1) для реального процесса (объекта) предполагает дискретность входных параметров, являющихся результатами измерений, экспериментов и т. д. Кроме того, обработка (1) с использованием современных вычислительных средств и численных методов так или иначе приведет к ее предварительной дискретизации. С учетом того, что функция (1) порождает m функций (2), имеет место следующее утверждение.

Утверждение 2. Произвольный ИП (ИО) может быть представлен в виде конечного множества $M_1, M_2,..., M_m$ матриц конечной размерности n с элементами из R, а анализ процесса принципиально можно свести к матричному анализу.

Замечание. Если в полученной совокупности $M_1, M_2,..., M_m$ $n > 2$, то любой матрице M_j, $j = \overline{1,m}$ можно поставить в соответствие конечное множество матриц размерности 2, каждая из которых получается из M_j путем фиксирования в ней всех индексов, кроме двух.

Пусть математической моделью ИО является матрица F ($n = 2$). Результат любых действий, производимых над объектом можно представить как возмущение ΔF матрицы F, а задача любого преобразования объекта – это задача получения возмущенной матрицы $\overline{F}$ для F, причем $\overline{F} = F + \Delta F$, где $\Delta F = f(F)$, то есть ΔF является некоторой функцией матрицы F, откуда вытекает истинность следующего утверждения.

Утверждение 3. Преобразования ИО эквивалентным образом представлены в виде элементарных матричных операций.

В качестве набора параметров, однозначно определяющих и всесторонне характеризующих любой ИО, можно использовать множество сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) специального вида соответствующей ему матрицы или, в случае ее симметричности, спектр и множество собственных векторов (СВ), являющиеся результатом нормального сингулярного (SVD) или спектрального разложения (СР) матрицы, которые однозначно определяют матрицу [3; 4], а значит и отвечающий ей ИО. Назовем такие наборы параметров полными. Любое преобразование объекта возмутит матрицу F, а значит и множества СНЧ и СНВ (СЗ и СВ).

Утверждение 4. Преобразование ИО эквивалентным образом представимо в виде совокупности возмущений СНЧ и (или) СНВ (СЗ и (или) СВ) его матрицы, что позволяет свести задачу анализа процесса преобразования и состояния объекта к анализу возмущений СНЧ и СНВ (СЗ и СВ).

Таким образом, на базе теории возмущений предложены основы единого подхода к анализу состояния ИО. Решение задач, связанных с оценками свойств ИО, сводится к анализу возмущений полных наборов параметров соответствующих матриц. Отсутствие в открытой печати аналогичных подходов в нашей стране и за рубежом делает результаты исследований приоритетными.

Литература: 1. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К.: Юниор, 2003. – 504 с. 2. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. – 430 с. 3. Кобозева А. А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах // Вісн. Східноукр. нац. ун-ту ім. В. Даля. – 2006. – №9(103). – Ч.1. – С. – 74 – 82. 4. Кобозева А. А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. – 2007. – №4.

УДК 004.056.53+004.057.4

Неласая А. В.

Козина Г. Л.

ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЦИФРОВОЙ ПОДПИСИ

Развитие технологий электронного документооборота требует новых механизмов обеспечения юридической силы коллективных электронных документов. В частности, при разработке коллективных проектов важной проблемой является использование протоколов [1–4], обеспечивающих реализацию коллективной электронной цифровой подписи.

В качестве источника абелевой группы для протокола коллективной подписи на основе ДСТУ-4145, предложенного в источнике [4], можно взять группу дивизоров гиперэллиптической кривой. Основное преимущество использования гиперэллиптических кривых состоит в том, что размер основного поля, над которым определена кривая, уменьшается пропорционально роду кривой без потери стойкости, хотя сама формула группового сложения выглядит более громоздко.

Протокол электронной цифровой подписи с предвычислениями ECPR был предложен с целью уменьшения трудоемкости операции верификации подписи в корпоративной сети за счет умножения только на базовую точку, которое можно выполнить с предвычислениями. Модифицируем этот протокол для реализации коллективной подписи.

Введем обозначения:

P – базовая точка эллиптической кривой;

l – количество пользователей;

n – порядок циклической подгруппы точек эллиптической кривой;

d_i – секретный ключ i-го пользователя;

h – хэш-образ сообщения;

$\pi(R) = X_R \bmod n$ – выделение x-координаты точки R = (X_R, Y_R) эллиптической кривой.

Генерация открытого коллективного ключа

1. Каждый i-й пользователь (i = 1..l) формирует открытый ключ вида:

$$Q_i = -d_i P \cdot$$

2. Коллективный открытый ключ вычисляется как сумма открытых ключей группы из l пользователей:

$$Q = \sum_{i=1}^{l} Q_i = \sum_{i=1}^{l} -d_i P \cdot$$

Формирование коллективной подписи

1. Каждый i-й пользователь (i = 1..l) рассчитывает точку R_i следующим образом:

а) выбирает случайный параметр $k_i, 1 < k_i < n$;

б) вычисляет значение $t_i = \frac{k_i}{h} \bmod n$;

в) и точку $R_i = t_i P$.

2. По представленным пользователями точкам R_i вычисляется общая точка:

$$R = \sum_{i=1}^{l} R_i = (X_R, Y_R).$$

3. И значение $w = \pi(R) = X_R \bmod n$.
4. Формируется точка $wR = (x, y)$,
5. И первая часть коллективной подписи

$$r = \pi(x, y) = x \bmod n.$$

6. Каждый пользователь вычисляет свой параметр s_i

$$s_i = (wk_i + hd_i) \bmod n$$

7. И предоставляет его для вычисления второй части коллективной подписи:

$$s = \sum_{i=1}^{l} s_i .$$

Коллективной подписью является пара чисел − (r,s).
Проверка коллективной подписи
1. Проверяющий вычисляет хэш-образ h' общего сообщения.

2. И значение $t = \frac{s}{h'} \bmod n$.

3. Используя открытый коллективный ключ Q, формирует точку $tP + Q = (x, y)$.

4. И вычисляет значение $v = \pi(x, y) = x \bmod n$.

5. Если $v = r$, то подпись признается подлинной.

Представленный протокол основан на предложенном недавно способе формирования и проверки подлинности коллективной цифровой подписи, базирующейся на понятии общего (коллективного) открытого ключа. Он обладает тем качеством, что размер подписи не увеличивается пропорционально числу подписавших участников, а при использовании гиперэллиптических кривых даже уменьшается пропорционально роду кривой. В дальнейшем необходимо рассмотреть вопросы стойкости предложенной схемы к различным типам атак.

Литература: 1. Min-Shiang Hawng. Research issues and challenges for multiple digital signature/ Hawng Min-Shiang, Le Cheng-Chi. // Int. J. of Network Security. – 2005. – Vol. 1. – №1. – P. 1 – 7. 2. Молдовян Н. А. Новые протоколы слепой подписи/ Н. А. Молдовян , П. А. Молдовян // Безопасность информационных технологий. – 2007. – №3. – С. 17 – 21. 3. Гортинская Л. В. Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310-95 и ДСТУ 4145-2002 / Л. В. Гортинская, Н. А. Молдовян, Г. Л. Козина // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2008. – №1. – С. 21 – 25. 4. Nelasa Anna. Digital Signature Protocol for corporate network / Anna Nelasa, Victor Dolgov, Anatolij Pogorily // Proceedings of International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2008). – Lviv-Slavsko (Ukraine). – 2008. – P. 396 – 397.

Трифонова Е. А.

УДК 004.056.5:518

МЕТОД ОБНАРУЖЕНИЯ ФАЛЬСИФИКАЦИИ ЦИФРОВОЙ ФОТОГРАФИИ

Развитие технических средств генерации цифровых изображений (ЦИ) привело к возможности массового использования недорогих с высокой разрешающей способностью цифровых видеокамер. Наряду с общедоступностью редактирующего изображения программного обеспечения и последними успехами в технике синтеза изображений это делает необыкновенно легким возможность манипулирования и переделки ЦИ, в силу чего чрезвычайно актуальной становится задача доказательства подлинности и обнаружения фальсификации ЦИ, в частности фотоснимков.

Важность рассматриваемой задачи для современной человеческой жизнедеятельности заставляет множество ученых искать пути и методы ее решения [1; 2]. Каждый из предлагаемых методов имеет, как правило, свою область применения. Большинство из методов не гарантируют обнаружение фальсификации ЦИ при ее наличии, а при обнаружении − не локализуют ее область.

Это заставляет искать новые математические инструменты и подходы к решению рассматриваемой задачи.

Целью работы является создание основ принципиально нового подхода к решению задачи обнаружения и локализации области фальсификации ЦИ, базирующихся на матричном анализе. Для достижения поставленной цели необходимо решить задачу установления характерных особенностей, отличающих матрицу исходного ЦИ от матрицы фальсифицированного ЦИ для конкретных способов фальсификации.

Будем считать, что в нашем распоряжении имеются фотоснимки, полученные современными цифровыми фотокамерами, то есть каждый из них − это полностью восстановленное после JPEG-сжатия изображение.

Пусть часть фотоснимка, который будем называть основным изображением (ОИ), заменяется частью ЦИ, далее называемой вклейкой, или замещающей областью (ЗО), хранящейся в формате без потерь. Такое фальсифицированное изображение (фотомонтаж) сохраняется без потерь.

Поскольку любая фальсификация ЦИ может рассматриваться как возмущение [3] матрицы изображения, а значит представляется как совокупность возмущений собственных значений (СЗ) и собственных векторов (СВ) исходной матрицы, однозначно определяемых ее нормальным спектральным разложением [4], то задачу можно конкретизировать следующим образом: необходимо установить характерные признаки этих возмущений (или свойства СЗ (СВ)), наличие или отсутствие которых даст возможность не только отделить фальсифицированное изображение от подлинного, но и локализовать область фальсификации.

Назовем матрицей нулевых собственных значений блоков (МНСЗБ) матрицу М размерности $[n/8]\times[m/8]$, где $[\bullet]$ – целая часть аргумента, значение каждого элемента которой определяется как количество нулевых СЗ в соответствующем блоке изображения, симметризованом согласно источника [5].

Очевидно, что для произвольного реального изображения, даже с учетом коррелированности значений яркости пикселей, вероятность того, что строки (столбцы) очередного блока окажутся линейно зависимыми, невелика, поэтому элементы МНСЗБ будут практически все нулевыми, чего нельзя утверждать для ЦИ, являющегося результатом восстановления после JPEG-сжатия. Это приведет к тому, что при построении МНСЗБ полученного фотомонтажа части, отвечающие ОИ и ЗО, будут отличаться по количеству нулевых СЗ блоков.

На основе идентификации этих различий предложен метод детектирования ЗО.

При формировании монтажа ОИ не учитывалось использование дополнительных операций обработки изображения для маскировки вклейки. Однако их применение не изменит характерных особенностей СЗ, выявленных выше, отличающих блоки ОИ от блоков ЗО, поскольку основа этих отличий лежит в том, что ОИ было сохранено с потерями, а вклейка без потерь. Заметим лишь, что размывка контура ЗО может привести к изменению картины полностью восстановленного после JPEG-сжатия изображения в областях ОИ, прилегающих к вклейке, что может помешать точному определению ее границы.

Предложенный метод рассматривает пока лишь частный случай фальсификации ЦИ, однако универсальность используемого подхода позволяет надеяться на возможность уйти в дальнейшем от конкретики фальсификации, анализируя лишь изменения СЗ матрицы изображения в результате возмущающего воздействия.

Литература: 1. Kundur D. Digital watermarking for tell-tale tamper proofing and authentication / D. Kundur, D. Hatzinakos // Proceedings of the IEEE. – 1999. – Vol. 87(7). – P. 1167–1180. 2. Bayram S. Image manipulation detection / S. Bayram, B. Sankur, N. Memon // Journal of Electronic Imaging. – 2006. – Vol. 15(4). – P. 1–17. 3. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. – 430 с. 4. Кобозева А. А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. – 2007. – №4. – С. 531 – 538. 5. Кобозева А. А. Использование нормального спектрального разложения симметричной матрицы в компьютерной стеганографии // Тр. Одес. политехн. ун-та. – 2007.– Вып.1(27). – С.185–190.

УДК 681.3.07

Степанов В. П.

Юхно И. А.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ЗАЩИТЫ СУБД ORACLE

Современный этап развития информационных систем характеризуется следующими особенностями [1 − 5]:

архитектура приложений, как правило, многозвенная − СУБД − сервер приложений − клиентская часть;

отдельные части приложений разработаны на разных программных платформах;

корпоративная информационная система является пространственно распределенной;

доступ в корпоративную информационную систему осуществляется при помощи технологий Интернет и Интранет.

Таким образом, современный этап развития информационных систем вызывает необходимость применения повышенных мер безопасности при работе с информационными системами. Рассмотрим реализацию политики безопасности, применяемой корпорацией Oracle. Основным продуктом корпорации в настоящее время является база данных, на основе которой создаются все другие приложения уровня корпорации. Следовательно, основное внимание необходимо сосредоточить на авторизированном подключении к информационной системе. Для этих целей Oracle применяет следующие средства:

авторизацию пользователей – пароль и профиль;

права на выполнение отдельных видов приложений – функций и процедур – с правами создателя или выполняющего;

создание виртуальной базы данных – VDB.

Рассмотрим более подробно особенности применения паролей в СУБД Oracle.

Парольная защита является наиболее распространенным способом аутентификации пользователей в современных информационных системах (ИС). Пользователь вводит пароль, сервер сравнивает значение, введенное пользователем с тем, что хранится у него в памяти и в зависимости от результата сравнения разрешает или отвергает подключение пользователя.

С хранением и передачей пароля связаны основные проблемы:

если передавать пароль в открытом виде, то его можно узнать, слушая пакеты по сети;

хранить пароль в сервере в открытом виде тоже небезопасно, так как его можно подсмотреть.

Таким образом, пароль приходится шифровать. Система шифрования паролей является достаточно консервативным элементом СУБД, ибо ее малейшее изменение влияет на возможность или невозможность подключения клиентов к базе данных. Таким образом, частое изменение этой подсистемы СУБД нежелательно. Видимо, этот фактор сказался на том, что подсистема шифрования паролей была неизменной много лет. Изменение системы шифрования повлекло бы за собой ряд сообщений ORA-xxxxx, сообщающих об ошибках в системе шифрования и в технической документации были бы упомянуты причины и способы их решения. Судя по отсутствию этих проблем в технической документации и Интернет.

Не обходимо отметить, что в СУБД Oracle не различаются строчные и заглавные символы (в версии Oracle 11g эта проблема устранена). Затем эксперименты с прослушиванием сетевых пакетов показали, что клиентский пароль не передается на сервер в открытом виде. Следовательно, обработка клиентского пароля осуществляется на клиенте, и для защиты пароля используется алгоритм шифрования. Скорее всего, этот алгоритм – DES, поскольку другого общедоступного сертифицированного алгоритма, существовавшего на протяжении последних 15 лет в США, нет.

Очевидно, что в СУБД Oracle на все инсталляции используется один и тот же ключ, потому что шифрование осуществляется на клиенте, но при этом клиент может подключаться ко всем базам данных, независимо от аппаратной платформы, битности, версий ОС и версий Oracle. Иными словами, проинсталлировав клиента у себя в ПК под Windows, можно подключаться к любой базе данных Oracle. Значит, значение ключа не является функцией, зависящей от версии СУБД, типа инсталляции (клиент или сервер), версии ОС. Очевидно, что сам собой напрашивается вывод о том, что ключ является константой, единой на все инсталляции СУБД, а значение этой константы "зашито" в каждом дистрибутиве, и даже конкретно в каждом исполняемом файле sql*plus

Согласно источника [1], подобная криптосистема – это ошибка с точки зрения криптографической защиты.

Последним штрихом для создания полноценной картины явилось опубликование 18 октября 2005 г. исследования " An Assessment of the Oracle Password Hashing Algorithm " авторов Joshua Wright и Carlos Cid, в котором описан алгоритм шифрования паролей в СУБД Oracle.

Можно сделать вывод, что:

реальной уязвимости на сегодняшний день Oracle не продемонстрировано. Каких-либо уязвимостей в криптографической конструкции не предъявлено. Новых теоретических результатов по вопросу получения несанкционированного доступа к СУБД Oracle тоже нет. Результаты по подбору паролей в [1; 3] получены за счет эффективного применения вычислительных средств и осуществляют банальную силовую атаку на хэш. При отсутствии специализированного ПО либо специализированных аппаратных средств, осуществить такую атаку за разумное время невозможно, точнее вероятность успеха ничтожно мала, а время атаки космически велико;

это подтверждается самими авторами [1], которые не нашли уязвимость в криптосхеме или ее реализации, а всего лишь продемонстрировали очередной силовой вариант. Надо отдать им должное, они честно признают этот факт: "…нельзя сразу указать криптографическую слабость конструкции хэш-функции в СУБД Oracle …" Фактически они подтвердили, что единственный способ на сегодняшний день узнать пароль – это силовая атака (полный перебор);

стойкость парольной защиты Oracle также подтверждается и известным сайтом, посвященном уязвимостям в СУБД Oracle: " It is not possible to decrypt a hashstring … ";

тем не менее, стоит подчеркнуть, что в системах с повышенными требованиями к безопасности для обеспечения надежной аутентификации следует использовать более сильные средства, чем стандартная парольная защита СУБД Oracle;

пользователям можно порекомендовать выбирать пароли, состоящие из нестандартных символов, заключая их в двойные кавычки.

Литература: 1. Wright Joshua. An Assessment of the Oracle Password Hashing Algorithm / Joshua Wright, Cid Carlos. – 18 oct., – 2005. 2. Брюс Шнайер. Прикладная криптография. – М.: Изд. "Триумф, 2003. – 816 с. 3. Morris R. Password security: A case history / R. Morris, K. Thompson // Communications of ACM. – V. 22. – №11. – Nov. 1979. – P. 594 – 597. 4. Хоффман Л. Дж. Современные методы защиты информации. – М.: Сов. радио, 1980. – 264 с. 5. Танненбаум Э. Современные операционные системы. – М. СПб.: Питер, 2002. – 1040 с.

УДК 65.012.8

Носов В. В.

Манжай О. В.

ДЕЯКІ АСПЕКТИ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ УКРАЇНИ

Розвиток інформаційних технологій зумовлює прогрес в усіх сферах людського життя. Нинішнє покоління людства стає свідком поступового переходу від індустріального суспільства до постіндустріального, однією з концепцій якого є так зване інформаційне суспільство. Збільшення ролі інформації в житті світової спільноти, звичайно, призводить до підвищення вимог щодо її захисту. Особливого значення захист інформації набуває в такій чутливій царині, як банківська сфера. І це не є випадковим. Адже стан банківської сфери впливає не тільки на економічну безпеку держави, але й безпосереднім чином на повсякденне життя пересічних громадян.

Дослідження вимог щодо організації системи захисту інформації в банківській сфері України показало, що на даний момент у цій царині існує велика кількість різнорідних нормативно-правових документів, які потребують системного упорядкування та доповнення з точки зору відомих підходів до організації захисту інформації.

Аналіз наявних у відкритому доступі нормативних документів [1 – 24], які тим чи іншим чином регламентують захист інформації в банківській галузі України, дозволив систематизувати їх з точки зору загальних підходів до організації захисту інформації. Така систематизація вибудовується шляхом формулювання нижченаведених питань, відповіді на які дають наявні нормативні документи [1 – 24].

Яка інформація відповідно до законодавства є об'єктом захисту? [1; 14; 15]

Який орган визначає політику захисту інформації в банківській системі України? [2]

Яка інформація в банківській системі становить державну таємницю? [16]

Яка інформація належить до банківської таємниці? [3]

Яка юридична відповідальність передбачена за порушення банківської таємниці? [8; 9; 10]

Які вимоги Національного банку України щодо захисту банківської таємниці? [20]

Як законодавчо визначено поняття електронних документів і передбачено їх обіг в інформаційно-телекомунікаційних системах? [6; 11]

Який правовий статус електронного цифрового підпису і відносин, що виникають при його використанні? [7; 12; 17]

Як законодавством визначені правила захисту інформації в інформаційно-телекомунікаційних системах? [4]

Які вимоги захисту електронних банківських документів для банків-учасників системи електронних платежів Національного банку України? [5; 18; 19; 21; 22; 24]

Чи потрібно ліцензування діяльності у сфері криптографічного захисту інформації в банківській системі України? [23]

Проведений аналіз у контексті організаційно-технічних аспектів системи захисту інформації в банківській галузі України дозволив сформулювати наступні завдання щодо вдосконалення організації захисту банківської інформації.

1. Необхідно розробити типове положення про службу захисту інформації в автоматизованій системі банку, яке уточнює положення НД ТЗІ 1.4-001-2000. "Типове положення про службу захисту інформації в автоматизованій системі" з урахуванням специфіки діяльності банків.

2. Доцільно розробити нормативно-методичні документи, що визначають основний перелік інформаційних загроз для банківської інформації (модель загроз) та методики оцінки вразливостей і ризиків для системи автоматизації банків.

3. Для отримання відповідних формальних гарантій захисту інформації системи обробки електронних банківських документів (платіжні системи) потребують сертифікації, наприклад, щодо відповідності міжнародному стандарту ISO/IEC 15408 "Загальні критерії оцінки безпеки інформаційних технологій".

4. З існуючих нормативних документів не зрозуміла легітимність цифрових підписів електронних банківських документів, тобто яким є статус центра сертифікації ключів Департаменту інформатизації НБ України, і входить він чи ні в схему взаємодії суб'єктів правових відносин у сфері послуг електронного цифрового підпису. Очевидно, що такий центр повинен бути в цій системі (принаймні для взаємодії з державними банками).

Література: 1.Закон України "Про інформацію" від 02.10.1992 (зі змінами та доповненнями на 23.06.2005) // Відомості Верховної Ради України. – 1992. – № 48 (01.12.1992). – ст. 650. 2. Закон України "Про Національний банк України" від 20.05.1999 (зі змінами та доповненнями на 09.07.2007) // Відомості Верховної Ради України. – 1999. – № 29 (23.07.1999). – Ст. 238. 3. Закон України "Про банки і банківську діяльність" від 07.12.2000 (зі змінами та доповненнями на 27.04.2007) // Відомості Верховної Ради України. – 2001. – № 5 – 6 (09.02.2001). – Ст. 30. 4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 20.05.1999 (зі змінами та доповненнями на 31.05.2005) // Відомості Верховної Ради України. – 1994. – № 31 (02.08.1994). – Ст. 286. 5. Закон України "Про платіжні системи та переказ коштів в Україні" від 05.04.2001 (зі змінами та доповненнями на 27.04.2007) // Відомості Верховної Ради України. – 2001. – № 29 (20.07.2001). – Ст. 137. 6. Закон України "Про електронні документи та електронний документообіг" від 22.05.2003 (зі змінами та доповненнями на 31.05.2005) // Відомості Верховної Ради України. – 2003. – № 36 (05.09.2003). – Ст. 275. 7. Закон України "Про електронний цифровий підпис" від 22.05.2003 // Відомості Верховної Ради України. – 2003. – № 36 (05.09.2003). – Ст. 276. 8. Цивільний кодекс України від 16.01.2003 (зі змінами та доповненнями на 31.05.2007) // Офіційний вісник України. – 2003. – № 11 (28.03.2003). – Ст. 461. 9. Кодекс України про адміністративні правопорушення від 07.12.1984 (зі змінами та доповненнями на 01.01.2008) // Відомості Верховної Ради УРСР. – 1984. – додаток до № 51. – Ст. 1122. 10. Кримінальний кодекс України від 05.04.2001 (зі змінами та доповненнями на 01.10.2007) // Відомості Верховної Ради України. – 2001. – № 25-26 (29.06.2001). – Ст. 131. 11. Постанова КМ України № 680 від 26 травня 2004 р. "Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу" (зі змінами та доповненнями на 08.12.2006) // Офіційний вісник України. – 2004. – № 21 (11.06.2004). – Ст. 1428. 12. Постанова КМ України № 903 від 13 липня 2004 р. "Про затвердження Порядку акредитації центру сертифікації ключів" (зі змінами та доповненнями на 08.12.2006) // Офіційний вісник України. – 2004. – № 28 (30.07.2004). – Ч. 1. – Ст. 1884. 13. Постанова КМ України № 377 від 29 березня 2006 р. "Деякі питання здійснення розрахунків за продані товари (надані послуги) з використанням спеціальних платіжних засобів" // Офіційний вісник України. – 2006. – № 13 (12.04.2006). – Ст. 882. 14. Постанова КМ України № 1126 від 08.10.97 р. "Концепція технічного захисту інформації в Україні" // [Електронний ресурс] / Ліга:Еліт: Мережна версія. 15. Указ Президента України № 1229 від 27.09.99 р. "Про затвердження положення про технічний захист інформації в Україні" (зі змінами та доповненнями на 06.10.2000) // Офіційний вісник України. – 1999. – № 39 (15.10.1999). – Ст. 1934. 16. Наказ Служби безпеки України від 12 серпня 2005 року № 440. "Про затвердження Зводу відомостей, що становлять державну таємницю" (зі змінами та доповненнями на 28.12.2007) // Офіційний вісник України. – 2005. – № 34 (09.09.2005). – Ст. 2089. 17. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України 13.01.2005 № 3 "Про введення в дію нормативного документу "Про затвердження Правил посиленої сертифікації" (зі змінами та доповненнями на 10.05.2006) // Офіційний вісник України. – 2005. – № 5 (18.02.2005). – Ст. 288. 18. Постанова Правління Національного банку України № 112 від 2 квітня 2007 року "Про затвердження Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України" // Офіційний вісник України. – 2007. – № 31 (07.05.2007). – Ст. 1250. 19. Постанова Правління Національного банку України № 243 від 4 липня 2007 року "Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи" (зі змінами та доповненнями на 29.12.2007) // Офіційний вісник України. – 2007. – № 62 (31.08.2007). – Ст. 2443. 20. Постанова Правління Національного банку України "Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці" № 267 від 14 липня 2006 року (зі змінами та доповненнями на 09.11.2006) // Офіційний вісник України. – 2006. – № 32 (23.08.2006). – Ст. 2330. 21. Постанова Правління Національного банку України № 320 від 16 серпня 2006 року. "Про затвердження Інструкції про міжбанківський переказ коштів в Україні в національній валюті" (зі змінами та доповненнями на 16.11.2006) // Офіційний вісник України. – 2006. – № 36 (20.09.2006). – Ст. 2507. 22. Постанова Правління Національного банку України № 620 від 10 грудня 2004 року. "Про затвердження Правил Національної системи масових електронних платежів" // Офіційний вісник України. – 2005. – № 2 (28.01.2005). – Ст. 93. 23. Лист Національного банку України № 24-112/876 від 31.05.2005 р. "Щодо ліцензування діяльності у сфері криптографічного захисту інформації в банківській системі України" // [Електронний ресурс] / Ліга:Еліт: Мережна версія. 24. Лист Національного банку України № 25-312/1359-6378 від 19.06.2006 р. "Щодо безпеки ринку платіжних карток в Україні" // Офіційний вісник нормативно-правових актів з митної справи, фінансів, податків та бухгалтерського обліку. – 2006. – № 26. – 6 червня.

УДК 37:004.73:004.056

Ковальчук В. Н.

ТИПОВА ПОЛІТИКА БЕЗПЕКИ НАВЧАЛЬНО-КОМП'ЮТЕРНОГО КОМПЛЕКСУ ПО ВІДНОШЕННЮ ДО КОРИСТУВАЧІВ-УЧНІВ

Основною вимогою до освітніх мереж є їх безперебійна робота. Навчальні комп'ютерні комплекси (НКК) не є захищеними від дестабілізуючих впливів, які можуть порушити працездатність їх програмного компонента. Поєднання двох проблем цих мереж: великої кількості недосвідчених користувачів і недостатності засобів захисту, роблять ці мережі особливо вразливими.

Завданням цієї статті є уточнення організаційних засад управління безпекою НКК через розробку типової політики безпеки загальноосвітнього навчального закладу по відношенню до користувачів-учнів.

НКК використовується в основному для навчальних цілей. Під цим слід розуміти, що апаратно-програмна складова НКК має забезпечувати якісний безперервний процес навчання, а це можливо лише за умови створення комплексної системи захисту інформації та інформаційних ресурсів навчального комп'ютерного комплексу загальноосвітнього навчального закладу. Впровадження такої системи неможливо без продуманої політики безпеки роботи з користувачами-учнями.

Політика інформаційної безпеки – набір законів, правил, практичних рекомендацій і практичного розвитку, що визначають управлінські та проектні рішення у сфері захисту інформації [1, с. 101].

Концепція політики безпеки повинна містити опис "моделей порушників і моделей їх поводження". Під порушником, зазвичай розуміють людину, яка "прагне реалізувати загрозу" [2, с. 25]. В даному випадку під порушником будемо розуміти користувача системи (учня), який своїми навмисними чи ненавмисними діями може завдати їй шкоди. *У неформальній моделі порушника,* як правило, намагаються передбачити основні мотиви діяльності порушника та частоту їх проявів.

Найбільш часто виникають помилки, тобто ненавмисні дії користувача, які все ж можуть завдати шкоди системі. Можливими також є навмисні дії, основним мотивом яких є цікавість. Останніми є власне зловмисні дії, що зустрічаються найрідше, але шкода від них найбільша. Мотиви зловмисних дій можуть бути різними. Виховні заходи є обов'язковими як для їх попередження, так і при реакції на їх скоєння.

Необхідно також розробити *стратегію адміністрування* користувачів, виходячи перш за все з наявних програмно-технічних засобів. Ці стратегії можна класифікувати за рівнем персоналізації:

повна – кожен учень чи інший користувач відповідно ідентифікується системою. Права розподіляються або за групами, або індивідуально;

часткова – користувачі НКК ідентифікуються за належністю до групи. Наприклад: учні, вчителі, лаборанти. Права розподіляються за групами;

відсутня – користувачі ніяк не ідентифікуються системою. Усі користувачі мають рівні права доступу до будь-якого ресурсу.

Основна мета політики безпеки НКК – це забезпечення виконання учнями-користувачами правил інформаційної безпеки, які унеможливлюють чи зводять до мінімуму шкоду, що вони можуть спричинити своїми діями, навмисними чи ненавмисними, програмному компоненту НКК. Ця мета реалізується організаційними, програмно-апаратними та виховними заходами.

Комплексний підхід до інформаційної безпеки вимагає поєднання таких заходів по відношенню до користувачів-учнів: контроль з боку вчителя (перш за все візуальний), контроль і реагування на несанкціоновані дії (НСД) програмних засобів захисту, реагування персоналу, вчителя при виникненні НДС і застосування відповідних виховних заходів. Під несанкціонованими діями, будемо розуміти дії, що заборонені політикою безпеки і конкретизовані в правилах користувачів.

До *організаційних заходів* належать перш за все розробка, впровадження та контроль за виконанням політики безпеки СЗІ НКК по відношенню до користувачів – учнів (ці правила доводяться до відома учнів у вигляді правил поведінки учнів). Контроль за виконанням покладено на вчителів та обслуговуючий персонал.

Програмно-апаратні заходи прийнятої політики безпеки реалізуються через систему управління (контролю) доступу користувачів до ресурсів, яка включає ідентифікацію та автентифікацію користувачів, управління (контроль) доступу до ресурсів, протоколювання та аудит дій користувачів. У правилах розмежування доступу необхідно заборонити доступ цих користувачів до системних областей диска, а також заборонити модифікацію ними програмного забезпечення, навчальної та іншої важливої інформації.

Основними в реалізації політики безпеки НКК є виховні заходи. Оскільки вони використовуються як для попередження НСД, так і для впливу на порушників правил безпеки, з метою їх перевиховання.

Політика безпеки роботи з користувачами-учнями з педагогічної точки зору повинна сприяти вихованню учнів, зокрема преміювати (розширювати права) за гарну поведінку і "карати" за погану поведінку. Основні методи, які використовують для безумовного виконання політики безпеки користувачами є: спонукання, попередження, тимчасова заборона (відмова в доступі), зменшення наданих прав і привілеїв (як користувача НКК) та ін.

Головна мета виховних заходів є усвідомлення учнями відповідальності за свої дії навіть у "віртуальному" середовищі, засвоєння етичних норм поводження в цьому середовищі, результатом чого є формування в учнів компетентності з інформаційної безпеки.

Література: 1. Лужецький В. А. Основи організаційного захисту інформації. Навч. посібник / В. А. Лужецький, Л. І. Северин, П. Ю. Гульчак, А. Д. Кожухівський. – Вінниця: ВНТУ, 2005. – 148 с. 2. Пономаренко В. С. Основи захисту інформації. Навч. посібник / В. С. Пономаренко, І. В. Журавльова, В. В. Туманов. – Харків: Вид. ХДЕУ, 2003. – 176 с.

Белодед Н. И.

Завиленская Т. П.

УДК 004.056

МЕХАНИЗМЫ ЗАЩИТЫ ОТ СОЦИАЛЬНОГО ИНЖИНИРИНГА

В любой организации есть уязвимые места [1]. Они есть всегда и заключаются не в системах, а в человеческом факторе. В этой связи следует обратить внимание на метод (атак) несанкционированного доступа к информации или системам хранения информации без использования технических средств, то есть социальный инжиниринг. Данный метод основан на использовании особенностей человеческой природы и считается достаточно деструктивным.

Социальный инжиниринг [2] используется довольно часто, особенно для проделывания взломщиком "тонкой работы" по краже документов и т. д. Данный феномен развивается в настоящее время как отдельная отрасль психологии.

Особенность метода заключается в том, что человек ничего не замечает. Это самый опасный тип атаки, который трудно обнаружить, а еще труднее от него защититься. Социальный инженер, использующий искусство обмана в качестве главного оружия, основывает свои действия на самых лучших человеческих качествах: стремлении помочь ближнему, вежливости, желанию работать в команде, отзывчивости и естественном желании довести дело до конца.

Цели могут быть самыми разными, но подразумевается один смысл. Этим смыслом и является кража информации. Те, кто использует социальный инжиниринг, претендуют на то, чтобы без лишнего внимания заполучить информацию, как правило, сделав копию. Далее осуществляются задуманные действия: продажа, перепродажа, шантаж первичного владельца и т. д. Тем не менее статистика говорит о том, что так тонко работают в большинстве случаев по заказу конкурирующей организации и т. п. [3].

Наиболее популярными инструментами атак являются:

Human denial of service (HDoS) (в переводе человеческий отказ в обслуживании, суть − заставить человека не реагировать на те или иные ситуации);

техническая социальная инженерия (здесь используются принципы и стереотипы социума);

звонок (подразумевается непосредственный голосовой контакт);

личный визуальный контакт (необходимо найти к жертве подход, вычисляется это с помощью анализа его вопросов);

электронная почта (e-mail);

системы обмена мгновенными сообщениями (MSN, ICQ, Skype и др.).

В случае социального инжиниринга, так же, как и в обычных атаках, целесообразно учитывать классификационные характеристики степени доступа при успешно проведенной атаке. Эта степень зависит от уровня подготовленности злоумышленника и того, кем является жертва.

Традиционно различают четыре уровня, представленных в порядке убывания полномочий: администратор, начальник, пользователь, знакомый.

Основные психологические инструменты, лежащие в основе самых распространенных методов социальных инженеров:

вхождение в роль (социальный инженер обычно демонстрирует несколько характерных признаков той роли, которую он разыгрывает);

доверие − это одна из наиболее распространенных атак социальной инженерии, фундамент всего следующего в дальнейшем;

жертву заставляют играть определённую роль (социальный инженер часто вынуждает свою мишень играть непривычную роль, например, принуждая ее к подчинению своим агрессивным поведением или взывая к жалости);

сбивание с мысли (социальные инженеры стремятся вступить в контакт с мишенями, когда те находятся в случайном режиме размышлений, и удерживать их там);

момент согласия (создают момент согласия, делая целую серию запросов, начиная с совершенно безобидных);

потребность помогать (люди испытывают позитивные эмоции, когда помогают другим);

присвоение (если человек присваивает себе некую роль, другие люди ведут себя по отношению к нему в соответствии с этой ролью);

симпатия (часто используют тот факт, что все люди более охотно говорят "да" в ответ на запрос людей, которые им симпатичны);

страх (социальный инженер иногда убеждает свою жертву в том, что должны случиться ужасные вещи, − но эту катастрофу можно предотвратить, если действовать так, как предлагает атакующий);

реактивность − это естественный ответ человеческой психики на ситуацию, угрожающую свободе.

Защита от атак социальных инженеров требует целого комплекса скоординированных усилий. Очень важно информировать сотрудников организации об этих угрозах и обучать их тому, как противостоять им и не давать себя использовать в качестве пособника атакующих. В течение многих лет человеческий фактор был и остается самым слабым звеном в структуре информационной безопасности.

Литература: 1. Митник Кевин Д. Искусство вторжения. – К: АйТи-Пресс, 2005. – 158 с. 2. Мухин Ю. И. Наука управлять людьми. – К: Фолиум, 1995. – 271 с. 3. Татарова Г. Г. Социологические исследования. – К.: Социс, 2001. – 83 с. 4. Мелихов И. Н. Скрытый гипноз. – К.: Перемена, 2003. – 105 с. 5. Райцин В. Я. Моделирование социальных процессов. – К.: КомпьютерПресс, 2005. – 154 с. 6. Митник Кевин Д. Искусство обмана / Кевин Д. Митник, Вильям Л. Саймон. – К.: Компания АйТи, 2004. – 286 с. 7. Гуц А. К. Социальные системы / А. К. Гуц, В. В. Коробицын. – К.: Наследие, 2000. – 130 с.

УДК 681.528.54

Домарєв В. В.

СУЧАСНІ МЕТОДИЧНІ ТА ОРГАНІЗАЦІЙНІ ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЇ

Практика показує, що проблема безпеки інформаційних технологій (БІТ) складна, різнопланова і пов'язана з вирішенням широкого спектру завдань, таких, як: побудова раціональних методів і моделей оцінки рівня безпеки інформаційних ресурсів в системах управління органів державної влади, особливо силових структур, проведення аудиту та експертиз стану безпеки інформаційно-телекомунікаційних систем (ІТС) з метою оцінки ефективності заходів щодо захисту інформації, розроблення ефективних апаратних і програмних засобів для реалізації алгоритмів методів і моделей систем безпеки інформаційних технологій.

Відомо, що захисні заходи забезпечують конфіденційність, цілісність і доступність інформації, однак якщо для режимних державних організацій на першому місці конфіденційність, то для комерційних структур важливіша за все цілісність (актуальність) і доступність даних. Порівняно з державними, комерційні організації більш відкриті й динамічні, тому ймовірні загрози для ІТС, які вони використовують, відрізняються й кількісно, і якісно. До того ж, методи оцінки важливості різних аспектів безпеки в державних і комерційних структурах досить різні.

Існуючі методичні рекомендації [1] щодо захисту інформації в ІТС орієнтовані в першу чергу на розроблювачів інформаційних систем, а не на користувачів чи системних адміністраторів або менеджерів безпеки. Водночас з практичної точки зору більш важливі рекомендації, які дають не суворе оптимальне, а досить ефективне рішення щодо захисту інформації.

Сучасні методики не враховують постійної перебудови структури ІТС, що захищаються, та не містять практичних рекомендацій з формування режиму безпеки. Іншими словами, ці рекомендації не дають відповідей на два головних із практичної точки зору питання:

Як створювати розподілену корпоративну інформаційну систему, щоб вона відповідала вимогам безпеки інформації?

Як практично сформувати політику безпеки й підтримувати її в умовах постійної зміни конфігурації програмно-апаратних засобів й структури самої системи?

На відміну від методик технічного захисту інформації на окремих об'єктах інформаційної діяльності виникає потреба дослідження та впровадження сучасних підходів і методичного апарату для створення систем безпеки інформаційних технологій (СБІТ), які б враховували питання захисту складних процесів обробки інформації в корпоративних ІТС. Тому виникає потреба дослідження методології безпеки ІТ сучасних потреб.

Як основні тенденції розвитку сучасних методичних підходів до захисту інформації можна зазначити:

розвиток методик оцінки, які дозволяють простежити рух від єдиної шкали ранжирування вимог і критеріїв безпеки до множини незалежних приватних показників і введенню частково упорядкованих шкал;

зростання ролі вимог адекватності реалізації засобів захисту і політики безпеки, що свідчить про переважання "якості" забезпечення захисту над її "кількістю";

визначення функцій учасників процесу створення й експлуатації захищених систем, застосування відповідних механізмів і технологій оптимального розподілу відповідальності між усіма учасниками цього процесу.

На даному етапі в інформаційно-телекомунікаційних системах органів державної влади та місцевого самоврядування України багато уваги приділяється створенню комплексних систем захисту інформації [2]. Але процес проектування та впровадження зазначених систем захисту базується на застарілих методичних підходах технічного захисту інформації, коли особлива увага приділяється збереженню конфіденційності інформації з обмеженим доступом на окремих об'єктах інформаційної діяльності.

Натомість сучасний рівень розвитку інформаційних технологій передбачає сумісне використання ІТС різноманітних за структурою, призначенням та власністю. Ускладнення технологій обробки інформації призвело до появи нових видів загроз для процесів функціонування комп'ютерних систем. Збитки та руйнації, що є наслідком реалізації загроз інформаційним технологіям, набагато більші, ніж наслідки загроз витоку інформації технічними каналами.

Створення СБІТ має свої відмінні властивості, а саме:

глобальну мету функціонування з багаторівневим, складним комплексом взаємопов'язаних цілей;

велику кількість функціональних задач, різних за властивостями, що комплексно взаємодіють і складають велику багаторівневу систему;

складну, багаторівневу організацію матеріальних та інформаційних потоків взаємодії елементів організаційної структури системи;

алгоритми функціонування і управління системи з багаторівневим характером та складною динамікою.

При переході від методів проектування засобів технічного захисту інформації до складних систем безпеки виникає необхідність створення єдиної комплексної методології проектування та впровадження СБІТ, яка об'єднує у собі методи розробки підсистем, елементів та програмних механізмів захисту інформації [3].

У зв'язку з цим у розробці СБІТ, на відміну від розробки засобів технічного захисту інформації, більшу частину складають задачі системного проектування та аналізу. Це задачі декомпозиції, системного проектування різних властивостей систем безпеки, побудови математичних та системних моделей різного класу, комплексування проектних рішень, розробки технічних вимог до елементів систем, аналізу коректності проектних рішень і т. п.

Оскільки СБІТ має велику вимірність і багаторівневість, то провести об'єктивний та достовірний аналіз проектних рішень на етапах системного проектування без сучасних комп'ютерних технологій неможливо. Тому методологія та методи розробки системних етапів СБІТ повинні створюватись з урахуванням їхньої подальшої реалізації комп'ютерними засобами, що, у свою чергу, потребує їхньої формалізації та розробки нової інформаційної технології проектування.

Таким чином, нові види загроз інформаційним технологіям, складність і різнорідність сучасних ІТС потребує наукового дослідження та розробки системного підходу до вирішення проблем захисту інформаційних ресурсів шляхом розвитку методологічних, технологічних та організаційних основ створення відповідних систем безпеки інформаційних технологій.

Отже, розвиток методологічних, технологічних та організаційних основ створення систем безпеки інформаційних технологій з метою підвищення ефективності організаційно-технічних заходів на етапах проектування, впровадження та експлуатації СБІТ є актуальною і важливою проблемою. Дослідження цієї проблеми дозволить визначити методичні шляхи створення ефективних систем безпеки ІТ, що раціонально об'єднують різноманітні за властивостями засоби, заходи і методи захисту інформації.

Література: 1. Постанова КМ України "Концепція технічного захисту інформації в Україні" від 8 жовтня 1997 р. №1126 // Безопасность информации. – 1998. – №1. 2. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення // http:www.ick.com.ua /?lng=18sec=4. 3. Домарев В. В. Безопасность информационных технологий. Системный подход. – К.: ООО ТИД Диа Софт, 2004. – 992 с.4. Постанова КМ України "Положення про технічний захист інформації в Україні" від 9 вересня 1994 р. №632. // Запорізька правда України. – 1994. – № 12.

УДК 681.3.004

Петров А. А.

МОДЕЛЬ ВЕРОЯТНОСТНЫХ УГРОЗ И ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ

Система защиты информации в сетях общего пользования представляет собой комплексную систему, включающую аппаратно-программные средства и методы, а также организационно-правовые меры, которые позволяют предотвратить или в максимальной степени затруднить возможность реализации угроз информации. Для оценки эффективности такой системы необходимо иметь инструмент ее формального представления, в качестве которого выступает модель защиты информации [1].

Наиболее общей моделью формального описания системы защиты является модель системы безопасности с полным перекрытием, в которой определяется полный перечень объектов защиты и угроз информации, определяются средства обеспечения безопасности с точки зрения их эффективности и вклада в обеспечение безопасности всей телекоммуникационной системы [2].

С этой целью в модель вводится набор защищаемых объектов $O = \{O_j\}$ и набор угроз $T = \{T_j\}$, каждая из которых направлена на один или несколько защищаемых объектов. Множество отношений угроза–объект образует двухдольный граф, в котором ребро $< t,O >$ существует тогда и только тогда, когда угроза t является средством для получения доступа к объекту O.

Цель моделируемой системы защиты состоит в том, чтобы перекрыть все возможные ребра в графе $\{< T,O >\}$, то есть добиться, чтобы ни к одному объекту не было ни одного не перекрытого пути ни от одной угрозы. Это достигается введением третьего набора $M = \{M_k\}$, включающего средства обеспечения безопасности. В идеальной системе каждое средство $m_k \in M$ должно устранять, по крайней мере, одно ребро $< t,O >$ из графа $\{< T,O >\}$. Введение набора M средств обеспечения безопасности преобразует двухдольный граф $\{< T,O >\}$ в трехдольный граф $\{< T,M,O >\}$, содержащий дуги вида $< t,m >$ и $< m,O >$.

Таким образом, в защищенной системе любое ребро в форме $< t,O >$ определяет незащищенный объект. Здесь одно и то же средство обеспечения безопасности может перекрывать более одной угрозы и/или защищать более одного объекта. Описанная модель удовлетворяет также общую схему взаимодействий, включающую систему организационного управления, внешние и внутренние угрозы, а также среду взаимодействия между ними [3].

Для описания объектов защиты введем набор $O = \{o(t)\}$, описывающий состав защищаемых объектов. С учетом потоковой схемы описания систем защиты дополнительно в рассмотрение введем набор $C = \{c(r)\}$ (или $C = \{c(i,j)\}$), описывающий всевозможные связи (взаимодействия) между элементами объекта, где $c(i,j) = 1$, если есть связь между элементами $o(i)$ и $o(j)$, и $c(i,j) = 0$ в противном случае.

Очевидно, что такое описание объекта в виде произвольной сети $< O,C >$ является наиболее общим; однако для учета особенностей рассматриваемой модели и решения задач, связанных с получением оценок, необходимо, во-первых, для каждого элемента и связи иметь соответствующие характеристики (соответственно множества $H(O)$ и $H(C)$), и, во-вторых, для моделирования защиты принципиально важно различать качественно разные связи (информационные, управляющие и т. д.). Уточнение типа связей может быть осуществлено различными путями, например, в характеристиках связи $h(c)$ из множества $H(C)$, но для простоты формулировки модели введем список связей $C = [C_1,C_2,...,C_n]$, где $C_1,C_2,...$ соответствуют связям 1-го, 2-го и т. п. типов.

В терминах решаемой задачи описание внешней среды должно содержать не только описание внешних объектов, но и описание предполагаемого нарушителя. В простейшем случае нарушитель описывается множеством внешних воздействий (угроз) $T = \{t_i\}$ с соответствующими характеристиками $H(T) = \{h(t)\}$. В общем случае необходимо рассматривать различные типы внешних воздействий: $T_1,T_2,...$. Это соответствует различным целям нарушителя. Таким образом, в общем случае имеется список множеств: $T = \{t_i\}$ при $i = 1,...,N$, который описывается соответствующим списком характеристик $H(T)$.

Пусть возможные различные воздействия на элементы и связи объекта защиты (уязвимости) характеризуются соответственно множествами $U(O)$ и $U(C)$, где $U(O) = \{u(i)\}$ и $U(O) = \{u(i,j)\}$.

Аналогично возможность элемента (связи) проявить активность, то есть оказать некоторое воздействие, не предусмотренное технологией обработки информации (например, выход из строя элемента (связи) будет обозначаться $v(i)$ или $v(i,j)$ из множеств $V(O)$ и $V(C)$ соответственно, а

множества $V(O)=\{v(i)\}$ и $V(C)=v\{(i,j)\}$, в свою очередь, могут объединяться в список V, как это описано выше.

Как составляющие описания объекта, U и V для получения оценок должны обладать соответствующими наборами характеристик $H(U)$ и $H(V)$.

Предполагается, что угрозы должны образовывать пару с различными "уязвимостями" – u из множеств $U(O)$ и $U(C)$, то есть угроза со стороны нарушителя должна соответствовать уязвимости для образования пары (t,u).

Препятствовать распространению угроз могут как естественные ограничения, так и искусственные средства защиты. Таким образом, общее формальное описание системы защиты должно содержать список средств защиты $Z=\{z\}$ с соответствующими характеристиками $H=\{h(z)\}$. При этом каждое средство защиты z должно быть связано с соответствующим защищаемым элементом (элементами) объекта или связью (связями) между элементами [4].

Модель вероятностных угроз в сети общего пользования позволяет построить базовые модели защиты информации, моделирующие различные ситуации несанкционированного доступа посредством сетей общего пользования.

Литература: 1. Петренко С. А. Аудит безопасности в Internet / С. А. Петренко, А. А. Петренко. – М.: ДМК Пресс. 2002 – 416 с. 2. Общие критерии оценки безопасности информационных технологий. Учебное пособие. Пер. с англ. Е. А. Сидак; [Под ред. М. Т. Кобзаря, А. А. Сидака. – М.: МГУЛ, 2001 – 84 с. 3. ISO/IEC 15408-1: Information technology – Security techniques – Evaluation criteria for IT Security-Post 1: Introduction and general model, 1999 // http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail.htm? csnumber =40612. 4. ISO/IEC 15408-2: Information technology – Security techniques – Evaluation criteria for IT Security-Post 1: Security functional requirements, 1999 // http://www.iso.org/iso/iso_catalogue/ catalogue_tc /catalogue_ detail.htm?csnumber=40613.

Астраханцев А. А.

Бондарь И. В.

УДК 681.3

КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА В СЕТЯХ СТАНДАРТА GSM. ПАКЕТНАЯ ПЕРЕДАЧА ДАННЫХ В СЕТЯХ СТАНДАРТА GSM С РАЗРАБОТКОЙ МЕХАНИЗМОВ ЗАЩИТЫ ТРАФИКА

Данная работа посвящена разработке методов защиты трафика в системах мобильной связи с коммутацией пакетов.

Рассматривается алгоритм шифрования AES (RIJNDAEL), который предлагается для использования в сотовой системе стандарта GPRS для обеспечения конфиденциальности ресурсов сети при шифровании IP-пакетов после прохождения SGSN, а также разработана программная реализация алгоритма на языке программирования C++.

Спектр услуг, предоставляемых операторами сотовой связи, непрерывно растет с целью привлечения большего числа абонентов. И одним из таких видов услуг является интеграция сотовых систем GSM в глобальную компьютерную сеть Internet при помощи перехода в режимы пакетной передачи данных, таких, как GPRS и EDGE. В настоящее время наиболее эффективные интеграционные технологии основываются на наборе протоколов IP. Это обуславливает необходимость адаптации мобильных сетей связи и мобильных технологий к функциональности технологии IP [1] .

В современных телекоммуникационных сетях внедряются методы, при которых любой вид информации преобразуется в цифровую последовательность, которая разбивается на отдельные фрагменты (пакеты) с прикрепленной к ним информацией по их идентификации, маршрутизации и коррекции ошибок. Это позволяет передавать единый информационный поток по различным средам распространения с применением универсальных систем коммутации. При этом на единой коммуникационной платформе решаются не только вопросы преобразования, коммутации и передачи информации, но и ее учета, хранения, а также управления сетями [2].

GPRS – это система, которая реализует и поддерживает протокол пакетной передачи информации в рамках сети стандарта GSM. При использовании системы GPRS информация собира-

ется в пакеты и через неиспользуемые в данный момент голосовые каналы, которые всегда есть в промежутках между разговорами абонентов, передается в эфир. Использование сразу нескольких голосовых каналов обеспечивает высокие скорости передачи данных. При этом этап установления соединения занимает несколько секунд. Таким образом, ресурсы сети используются более эффективно.

Система защиты сетей GSM-GPRS имеет серьезные недостатки на многих уровнях защиты, так как имеет уязвимости в различных частях сети оператора GSM. Саму систему нельзя признать удачной. Даже если применять стойкие алгоритмы шифрования, вся система все равно не защищена от различных "социальных" сценариев, например, если злоумышленник работает в компании-операторе [3].

Проанализировав вышесказанное, можно отметить, что наиболее уязвимым участком сети GPRS является не радиоучасток, хоть и алгоритмы шифрования, которые там применяются достаточно слабые, а участок, на котором радиопакеты преобразуются протоколом IP. Поэтому наиболее вероятными атаками на пакеты будут атаки на соединение между SGSN (Serving GPRS Support Node) и GGSN (Gateway GPRS Support Node), атака на сеть из GPRS-сети другого оператора или атака на сеть из Интернета [3]. Для предотвращения таких атак необходимо применять шифрование IP-пакетов стойкими криптографическими алгоритмами. В качестве такого алгоритма может быть AES (Advanced Encryption Standard − Rijndael). Алгоритм Rijndael является блочным шифром с переменным размером блоков и переменной длиной ключа. Размеры ключа и блоков могут независимо друг от друга принимать значения 128, 192 и 256 бит, что очень удобно при варьировании между скоростью шифрования (очень важна, так как радиоресурсы на сегодняшний день являются дорогостоящими) и необходимым уровнем гарантированности защиты пользовательских данных [4].

Для предотвращения атак необходимо применять шифрование IP-пакетов стойкими криптографическими алгоритмами. Была разработана программа для осуществления алгоритма шифрования Rijndael, которая может быть внедрена в систему связи для повышения ее безопасности.

С развитием технологий 128 битное кодирование не будет осуществлять гарантированной стойкости, поэтому целесообразно применять 256-битное кодирование [2].

Литература: 1. Гольдшшейн Б. С. Перспективные услуги сотовых сетей поколений 2,5 и 3G / Б. С. Гольдшшейн, В. А. Фрейкман, А. А. Витченко // Мобильные системы. – 2002. – № 5. – с. 8. 2. Громаков Ю. А. Стандарты и системы подвижной радиосвязи. — М.: Эко-Трендз, 1997. — 238 с. 3. Голикова Е. GPRS. Новое слово в мобильной связи // Мобильные системы. – 2002. – № 10. – С. 51. 4. Горбенко І. Д. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч. 1. Криптографічний захист інформації / І. Д. Горбенко, Т.О. Грінєнко. – Харків: ХНУРЕ, 2004. – 368 с. 5. Абрамов А. Стандарт GSM: строим систему сотовой связи // Мобильные системы. – 1999. – №3. – С. 30 – 36. 6. Бабков В. Ю. Системы мобильной связи / В. Ю. Бабков, М. А. Вознюк, В. И. Дмитриев. – СПб.: СПбГУТ, 1999. – 330 с. 7. Берездивин Р. Технологии и решения беспроводной связи следующего поколения / Р. Берездивин, Р. Брейнинг, Р. Топп // Мобильные системы. – 2002. – №7. – С. 18 – 26.

УДК 004.056

Белодед Н. И.

Петровская Н. А.

СЕТЕВЫЕ АТАКИ И ЗАЩИТА ОТ НИХ

Популярность Интернет сделала миллионы компьютеров по всему миру уязвимыми для возможных сетевых атак [1].

Атака − любое действие нарушителя, приводящее к реализации угрозы, путем использования уязвимостей сети либо компьютера.

Существуют четыре основных категории атак:

атака доступа − это попытка получения злоумышленником информации, для просмотра которой у него нет разрешений (например, "подсматривание", "подслушивание", "перехват");

атака модификации − это попытка неправомочного изменения информации (замена существующей информации, добавление новых данных, удаление существующих данных);

атаки на отказ от обязательств − это атаки, направленные против возможности идентификации информации, то есть попытка дать неверную информацию о реальном событии или транзакции ("маскарад", "DoS-атаки против Интернета", "отрицание события");

атаки на отказ в обслуживании (Denial-of-service, DoS) − это атаки, запрещающие легальному пользователю использование системы, информации или возможностей компьютеров. Более разрушительный тип DoS атаки − распределенная атака на отказ в обслуживании (distributed denial of service, DDoS). Данная атака осуществляется с множества компьютеров, находящихся в подчи-

---

нении злоумышленника. Атака может быть направлена на любое сетевое устройство: маршрутизаторы, серверы (Web, mail, DNS) или специфичные компьютеры (firewalls, IDS) [2].

Наиболее распространенные атаки данного типа: Ping-of-Death, WinNuke, Атака Land , SYN Flood, Land/Latierra , UDP bomb , Атака smurf и другие.

Наиболее распространенные способы защиты: самым популярным и доступным способом защиты от сетевых атак является брандмауэр.

Брандмауэр (файервол, межсетевой экран) – это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую [3].

Все брандмауэры можно разделить на три типа:

пакетные фильтры (packet filter);

сервера прикладного уровня (application gateways);

сервера уровня соединения (circuit gateways).

Все типы могут одновременно встретиться в одном брандмауэре.

В некоторых случаях одного брандмауэра недостаточно. Тогда прибегают к использованию системы обнаружения вторжений (СОВ, Intrusion Detection System (IDS)).

Существуют два основных типа IDS [4]:

узловые (HIDS) – располагается на отдельном узле и отслеживает признаки атак на данный узел;

сетевые (NIDS) – находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети.

Также используются и иные разновидности IDS, например:

ERIDS (External Routing Intrusion Detection System) занимается отслеживанием попыток перехвата сетевого трафика путем перенастройки маршрутизаторов для использования злоумышленником;

OIDS сравнивает действия конкретного пользователя в данный момент времени с его обычными действиями, и в случае сильных расхождений – сообщает об этом.

Две основные технологии построения СОВ [5]:

системы обнаружения аномального поведения (anomaly detection);

системы обнаружения злоумышленного поведения (misuse detection). Механизм функционирования системы обнаружения атак на уровне сети состоит из 4-х основных этапов:

захват пакетов;

фильтрация и сборка фрагментов;

распознавание атак;

реагирование на них.

Однако, какими бы надежными не казались технические и программные средства защиты, эффективность их работы зависит от правильной конфигурации, которую настраивает пользователь. Поэтому весьма важна роль знающих и опытных администраторов сети.

Литература: 1. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры. – К.: БИНОМ. Лаборатория знаний, 2004. – 421 с. 2. Оглтри Т. В. Firewalls: Практическое применение межсетевых экранов. – К.: ДМК Пресс, 2001. – 216 с. 3. Лукацкий А. В. Способы обхода межсетевых экранов / Научно-инженерное предприятие "Информзащита", 2002. – 252 с. 4. Данжани Н. Средства сетевой безопасности / Н. Данжани, Д. Кларк. – К.: КУДИЦ-Пресс, 2007. – 304 с. 5. Польман Н. Архитектура брандмауэров для сетей предприятия / Н. Польман, Т Кразерс. – К.: Вильямс, 2003. – 113 с. 6. Лебедь С. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – К.: МГТУ им. Н. Э. Баумана, 2003. – 118 с. 7. Митник К. Д. Искусство вторжения / К. Д. Митник, В. Л. Саймон. – К.: ДМК Пресс, 2005. – 29 с. 8. Аграновский А. В. Новый подход к защите информации — системы обнаружения компьютерных угроз / А. В. Аграновский, Р. А. Хади. – К., Ростов-на-Дону, 2007. – 54 с.

Емельянов С. Л.

УДК 621.391.82:621.396.6

ПРОБЛЕМНЫЕ АСПЕКТЫ БЛОКИРОВАНИЯ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Угрозы конфиденциальности информации, циркулирующей в современных информационных системах, по-прежнему являются одними из самых распространенных и опасных [1]. Поэтому актуальной является проблема выявления, анализа и блокирования современных технических каналов утечки информации (ТКУИ). В решении данной проблемы накоплен значительный опыт в части нормативно-методического и аппаратно-технического обеспечения защиты электромагнитных и электрических ТКУИ, обусловленных побочными электромагнитными излучениями и наводками (ПЭМИН) от работающих средств ЭВТ [2; 3].

Менее исследованными являются ТКУИ, образованные применением различных типов аппаратных закладок (АЗ). Основные проблемные аспекты здесь обусловлены априорной неопределенностью о видах и характеристиках применяемых АЗ. Ситуация усугубляется необходимостью аттестации не только средств ЭВТ, обрабатывающих информацию с ограниченным доступом, но и помещений, где они установлены [4; 5].

В качестве примера рассмотрены существующие методы активной (на базе сетевых генераторов шума) [6] и пассивной (на основе сетевых помехоподавляющих фильтров) [7] защиты электрических ТКУИ, образованных мощными узкополосными (кварцованными) сетевыми АЗ в целях аудиоконтроля выделенных помещений.

Показано теоретически и проверено экспериментально, что на выходе отечественных сертифицированных помехоподавляющих фильтров серии "М" (ЗАО "Сетевые технологии", г. Нетишин) и ФМПЗ (НТУУ "КПИ", г. Киев) в условиях априори неизвестной рабочей частоты сетевой АЗ [8] могут присутствовать остатки неподавленных информативных сигналов, величина которых на 7−10 дБ превышает пороговую чувствительность существующих разведприемников, что и обуславливает возможность утечки информации по такому каналу.

Таким образом, в данных условиях целесообразно сочетание активных и пассивных методов блокирования [9], предложено и исследовано реализующее устройство защиты.

Литература: 1. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб.: Питер, 2008. – 320 с. 2. Хорев А. А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи // Специальная техника. – 1998. – №2. – С. 41 – 46. 3. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К.: Юниор, 2003. – 504 с. 4. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М.: Горячая линия-Телеком, 2005. – 416 с. 5. Временные рекомендации по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам побочных электромагнитных излучений и наводок (ВР ЭВТ–95)// Безопасность информации. – 1995. – №2. – С. 54 – 57. 6. Емельянов С. Проблемные аспекты реализации пространственного и линейного зашумления в системах активной защиты информации / С. Емельянов, Н. Логвиненко, В. Носов, В. Писаревский // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – №2. – С. 135 – 138. 7. Емельянов С. Л. Эффективность фильтрации информативных сигналов в электрических каналах утечки информации // Труды восьмой международной научно-практической конференции "Современные информационные и электронные технологии". Одесса, 21 – 25 мая 2007 г. – Одеса. СИЭТ, 2007. – С. 179. 8. Емельянов С. Л. К вопросу выбора рабочего диапазона частот сетевых закладных устройств аудиоконтроля / С. Емельянов, В. Гаращук //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – №1(12). – С. 158 – 162. 9. Методы борьбы с сетевыми закладными устройствами // Матеріали третьої міжн. наук.-практ. конф. "Наукові дослідження – теорія та експеримент 2007" Т.7. Полтава,14 – 16 травня 2007 р. – Полтава: "ІнтерГрафіка", 2007. – С. 135.

УДК 007:330

Охрименко С. А.

Тутунару С. А.

Склифос К. Ф.

ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время информационное пространство современного общества объединяет информационные ресурсы, информационные технологии и информационную инфраструктуру предприятий и организаций, коллективных и индивидуальных пользователей. Наше общество постоянно сталкивается не только с проблемами экономического, социального и экологического характера, но и информационного. В среде комплекса информационных проблем ведущее место принадлежит информационной безопасности.

Проблема информационной безопасности носит комплексный характер и объединяет сочетание правовых, организационных и программно-технических мер. В последнее время отмечается пристальный интерес к экономическим аспектам информационной безопасности. Этот интерес

объясняется не только увеличением затрат на обеспечение информационной безопасности, которые отмечаются повсеместно, но и необходимостью представления экономических выкладок для разъяснения важности и целесообразности вложений в информационную безопасность для существующего бизнеса.

Экономика информационной безопасности (ЭИБ), как самостоятельное научное направление, получило развитие в 90-х годах прошлого столетия [1–6]. Истоками данного направления следует считать комплекс исследований и практических разработок, связанных с такими факторами, как:

процессы совершенствования организационных форм использования вычислительной техники;

замена вычислительной базы и переход к использованию новых информационных и коммуникационных технологий;

разработка операционных систем для персональных компьютеров;

появление специфических угроз (компьютерных вирусов);

реализация атак на информационные системы и др.

Идеальная система информационной безопасности должна объединять в себе комплекс мер, таких, как правовые, организационные, технические, экономические и морально-этические. Но создание именно идеальной системы возможно только по отношению к государственным информационным системам, чьи ресурсы защищаются специальными подразделениями. Применительно к деятельности коммерческих структур процессы проектирования, внедрения и эксплуатации СИБ сопряжены с огромными затратами, требуют наличия высококвалифицированных кадров и т. д., что является не всегда доступным.

В работе рассмотрены основные проблемы формирования ЭИБ как новой учебной дисциплины. Данная дисциплина, по мнению авторов, является на сегодняшний момент наиболее актуальной, поскольку специалисты уделяют все большее внимания вопросам экономической эффективности систем информационной безопасности. Отмечается общая тенденция роста стоимости работ по информационной безопасности, так как процессы проектирования, внедрения и эксплуатации системы информационной безопасности сопряжены с огромными затратами на программные и технические средства, требуют наличия высококвалифицированных кадров и т. д.

В рамках данного направления выделяются работы, связанные с исследованием комплекса показателей экономической эффективности, разработкой экономико-математических моделей, управлением риском и др. [7–9]. Необходимо детальное изучение методов расчета эффективности системы информационной безопасности, поскольку именно они характеризуют инвестиционную привлекательность. К их числу относят следующие:

суммарная стоимость владения TCO (Total Cost of Ownership);

чистая приведенная стоимость NPV (Net Present Value);

внутренняя норма рентабельности IRR (Internal Rate of Return);

экономическая привлекательность EVA (Economic Value Added);

сбалансированная балльная оценка BSC (Balanced Score-card).

Особое внимание, по мнению авторов, должно уделяться подготовке и разработке организационно-распорядительной документации, которая интегрирует теоретические знания и практические навыки, полученные в процессе освоения основных разделов данного предмета.

Представленный материал отражает только точку зрения авторов и не может претендовать на завершенность. Вполне очевидно, что данный предмет может быть дополнен новыми разделами, отражающими современные теоретические знания и практические навыки, используемыми для разрешения кризисных ситуаций в управлении системами информационной безопасности, а также соответствовать требованиям международных и национальных стандартов.

Литература: 1. Галицын В. К. Планирование на предприятиях информационно-вычислительного обслуживания / В. К. Галицын, С. П. Куценко, М. И. Кутер, С. Ф. Лазарева. – К.: Техника, 1991. – 221 с. 2. Герасименко В. А. Основы защиты информации в автоматизированных системах обработки данных. – М.: ВИНИТИ, N 1080-В-91, 1991. – 478 с. 3. Доветов М. Ш. Экономика и организация вычислительных установок / М. Ш. Доветов, В. А. Залесов. – М.: Финансы и статистика, 1982. – 303 с. 4. Новицкас Ю. М. Экономика ЭВМ. – Ленинград: Машиностроение, 1983. – 176 с. 5. Экономика индустрии информатики / Под ред. Ю. М. Каныгина, А. М. Меняйло. – Красноярск: Изд-во Краснояр. Ун-та, 1987. – 336 с. 6. Якушенко В. Г. Планирование, учет и анализ деятельности хозрасчетных вычислительных установок. – М.: Статистика, 1980. – 112 с. 7. Rachel Rue. A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. Rachel Rue, Shari Lawrence Pfleeger and David Ortiz // Workshop on the Economics of Information Security (2007). 8. Gritzalis S. A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments. / S. Gritzalis, A. N. Yannacopoulos, C. Lambrinoudakis, P. Hatzopoulos, S. K. Katsikas // Int. J. Inf. Secur. (2007) 6:197–211. 9. Sklavos Nicolas. Economic Models and Approaches in Information Security for Computer Networks / Nicolas Sklavos, Panagiotis Souras International Journal of Network Security. – Jan. 2006. – Vol.2. – №1. – P.14 – 20.

Секція 2
Захист інформації в комп'ютерних системах

УДК 681.322

Гавриш Т. В.

Тюпич Е. В.

VPN-РЕШЕНИЯ ПРИ ПРОЕКТИРОВАНИИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Одним из основных факторов, определяющих эффективность разрабатываемых корпоративных информационных систем (КИС), является обеспечение защищённого межсетевого взаимодействия авторизованных пользователей. Данная задача традиционно решается путём построения системы информационной безопасности (СИБ), которая должна функционировать абсолютно прозрачно для приложений КИС и быть полностью совместимой с используемыми в КИС техническими средствами и IT-технологиями [1]. Последнее может быть выполнено при условии интеграции разработки системы безопасности в процесс проектирования КИС.

Построение системы ИБ проводится как для функционирующей, так и для разрабатываемой КИС. В первом случае построение (модификация) СИБ осуществляется после аудита безопасности КИС, оценки рисков нарушения ИБ и является по существу выработкой контрмер по снижению рисков до допустимого уровня. Причем аудит может быть как плановым, так и специальным обследованием, представляющим собой анализ причин компьютерных инцидентов. Однако независимо от того создается или модифицируется СИБ, речь идет о встраивании средств защиты информации в уже существующую КИС. А это в условиях гетерогенной среды обуславливает необходимость согласования взаимодействия продуктов разных производителей.

При создании СИБ большинство разработчиков (например, [1, 2]) исходят из того, что проект КИС априорно известен, то есть спроектированная КИС дополняется средствами защиты информации. Следует отметить, что некоторые авторы [3] соглашаются, что проектирование КИС в изначально защищённом исполнении позволит учесть требования безопасности непосредственно в процессе её создания и в результате повысит структурированность, однородность и управляемость системы. Однако более обстоятельные рекомендации по технологии разработки системы ИБ в контексте этапов жизненного цикла КИС отсутствуют. По мнению авторов данной публикации, согласование проектных решений на всех этапах разработки и эксплуатации КИС с требованиями информационной безопасности позволит существенно повысить уровень защищённости информационных ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести ущерб владельцам и/или пользователям информации.

Следует отметить, что в большинстве распределённых КИС для передачи конфиденциальной информации используется Интернет, например, связь офиса предприятия с удалёнными сотрудниками. В этой ситуации основной угрозой информационной безопасности является несанкционированный доступ (НСД) к корпоративным данным в процессе их передачи по сети. Защита от НСД в Интернете может быть достигнута только на основе комплексного применения технологий сетевой безопасности, одной из которых является создание виртуальных защищённых сетей VPN, объединяющих методы туннелирования, шифрования и аутентификации.

Конфигурация и характеристики виртуальных частных сетей во многом определяются типом применяемых VPN-продуктов. В настоящей работе рассматриваются процедуры выбора технической реализации сетей VPN в зависимости от требований корпоративных заказчиков, заявленных при проектировании КИС, организационной структуры предприятия, соотношений технических характеристик и стоимости VPN-продуктов.

Существует обширный рынок коммерческих VPN-продуктов. Для построения VPN могут применяться следующие сетевые средства защиты:

серверы удалённого доступа, позволяющие создать защищённые туннели на канальном уровне модели OSI;

маршрутизаторы со встроенными функциями VPN, поддерживающие протоколы создания VPN на канальном и сетевом уровнях;

межсетевые экраны, включающие в свой состав серверы удалённого доступа;

автономное программное обеспечение;

специализированные аппаратные средства, ориентированные на формирование защищённых туннелей на канальном и сетевом уровнях.

При этом следует учесть, что проектируемая СИБ должна удовлетворять следующим требованиям:

интегрируемость с существующими сетевыми средствами (маршрутизаторами, межсетевыми экранами, ОС), а также интегрируемость различных информационных и сетевых технологий между собой для обеспечения комплексной защиты программных, информационных и технических ресурсов;

масштабируемость технических решений с учётом развития СИБ;

прозрачность работы VPN для всех внутрикорпоративных приложений;

недопустимость снижения пропускной способности защищаемой сети.

В заключении следует отметить, что предложенные изменения в технологии проектирования КИС с учетом требований по обеспечению ИБ обусловили возможность следующих интегрированных решений в части выбора программно-технических средств:

интеграция средств защиты с элементами КИС − маршрутизаторами, службами каталогов, операционными системами, серверами и пр.;

интеграция различных технологий безопасности между собой для обеспечения комплексной защиты ИС, например, интеграция межсетевого экрана с VPN-шлюзом.

Реализация указанных решений позволяет повысить уровень информационной безопасности, что весьма существенно в условиях сложной гетерогенной структуры современных КИС.

Литература: 1. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 616 с. 2. Петренко С. А. Новые инициативы российских компаний в области защиты информации / С. А. Петренко, С. В. Симонов // Конфидент. – 2003. – №1. – С. 34 – 39. 3. Бабков И. Н. Рекомендации по созданию корпоративной системы информационной безопасности / И. Н. Бабков, С. А. Лавров //Атомная стратегия. – 2004. – №12. – С. 17 – 21.

Дорохова Л. П.

Дорохов О. В.

УДК 657.1.011.56(075.8)

НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВНУТРІШНІХ МЕРЕЖ І САЙТІВ ФАРМАЦЕВТИЧНИХ ПІДПРИЄМСТВ

В умовах значного посилення конкуренції на фармацевтичному ринку України його учасники (вітчизняні виробники лікарських засобів, представництва закордонних фірм, оптові дистриб'ютори фармацевтичної продукції, аптечні заклади − кінцеві продавці ліків) змушені активно розвивати та впроваджувати у свою виробничо-комерційну діяльність сучасні інформаційні та Інтернет-технології [1 − 3].

Основними напрямками цього процесу є розробка та експлуатація внутрішніх корпоративних комп'ютерних систем, технологій та баз даних, а також створення та підтримка зовнішніх web-сайтів, спрямованих на вирішення комерційно-логістичних цілей та бізнес-завдань відповідних фармацевтичних підприємств [2 − 4].

Надзвичайної важливості при цьому набувають питання забезпечення належної інформаційної безпеки, яку слід розглядати як з точки зору загальновизнаних критеріїв та вимог до захисту комерційної та критично важливої управлінської інформації [5; 6], так і з урахуванням специфічних особливостей саме питань забезпечення інтересів і вимог споживачів лікарських засобів і товарів медичного призначення.

Стосовно внутрішнього інформаційного середовища фармацевтичних підприємств основними об'єктами, що потребують захисту та унеможливлення стороннього втручання є наступні:

бази даних різної функціональної спрямованості та змісту, які містять основну комерційну та закриту інформацію;

програмні та апаратні засоби забезпечення роботи внутрішніх локальних мереж, котрі повинні бути надійно захищені від зовнішнього несанкціонованого впливу або доступу;

програмні додатки та продукти, що функціонують на окремих комп'ютерах і забезпечують оперативне, в режимі реального часу вирішення їх користувачами − особами, що приймають рішення − управлінсько-виробничих завдань, а тому повинні працювати у штатних режимах, гарантовано коректно та достовірно за результатами.

Не менш важливими та актуальними є питання забезпечення інформаційної безпеки зовнішніх web-сайтів, незадовільне вирішення якого може суттєво негативно вплинути на взаємовідносини фармацевтичного підприємства − власника сайту зі своїми наявними та потенційними клієнтами, контрагентами, партнерами та замовниками.

Особливу увагу в цьому випадку слід приділити наступним завданням:

забезпечення недоторканності інформаційно-довідкової та нормативно-правової документації стосовно лікарських засобів (ліцензування, дозволів на застосування в Україні, юридично-правових аспектів торгівлі ними тощо);

захист від несанкціонованих зовнішніх коригувань комерційної інформації виробників, дистриб'юторів стосовно наявності лікарських препаратів у продажу, цінових та інших умов постачання і таке інше;

необхідність надійного постійного підтвердження та ідентифікації фактичної приналежності самого web-сайту, тобто запобігання можливості створення, або переключення на фішинговий (підроблений, підставний) сайт, яке може суттєво зашкодити не лише іміджу, репутації власника справжнього сайту, але й привести до прямої матеріальної, фізичної шкоди кінцевим споживачам лікарських препаратів − населенню;

унеможливлення фармінгу, тобто перенаправлення відвідувачів сайту за фальшивими або не потрібними їм Internet-адресами, що викликає у кращому разі роздратування користувачів, зайві та необґрунтовані витрати ними ресурсів, часу тощо;

забезпечення конфіденційності користування сайтом, в тому числі даних щодо відвідувачів сайту (їх електронних адрес, замовлених ними лікарських препаратів або тих, якими цікавився користувач сайту і таке інше).

Всі вищенаведені завдання є загальними для корпоративних інформаційних мереж і сайтів комерційних підприємств, але серед суб'єктів саме фармацевтичної галузі України вони до цього часу практично не розглядалися та належної уваги їм не приділялося.

Вирішення цих питань вимагає суттєвого збільшення уваги та залучення до їх розв'язання як спеціалістів з інформаційних технологій, так і фахівців-менеджерів фармацевтичних підприємств та організацій, що у кінцевому підсумку сприятиме вирішенню важливого суспільно-соціального завдання покращання забезпечення населення України лікарськими препаратами та товарами фармацевтичного призначення.

Література: 1. Про затвердження Державної програми забезпечення населення лікарськими засобами на 2004-2010 рр // Юридичні аспекти фармації. – 2003. – № 15. – С. 3 – 4. 2. Мнушко З. М. Розвиток логістичного моделювання діяльності оптових фармацевтичних підприємств на вітчизняному ринку / З. М. Мнушко, С. А. Куценко, Л. П. Дорохова // Фармац. журн. – 2005. – №5. – С. 3 – 7. 3. Черних В. П. Усвідомлення парадигми розвитку фармацевтичної галузі України / В. П. Черних, О. В. Посилкіна, Г. В. Зайченко // Вісник фармації. – 2005. – №1(41). – С. 3 – 9. 4. Пономаренко М. С. Канали доведення фармацевтичного продукту до кінцевого споживача/ М. С. Пономаренко, В. А. Загорій, В. В. Огородник // Фармац. журн. – 2001. – №5. – С. 23 – 27. 5. Филин С. А. Информационная безопасность. – М.: Альфа-Пресс, 2006. – 412 с. 6. Карминский А. М. Информатизация бизнеса: концепции, технологии, системы. – М.: Финансы и статистика, 2004. – 624 с.

УДК 681.511:3

Астраханцев А. А.

Вакуленко В. С.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ СКРЫТИЯ ИНФОРМАЦИИ В НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЯХ

Стеганография − скрытие (путем встраивания) сообщений в цифровых данных таких, как речь, изображение, аудио- или видеозаписи, текстовые файлы. Достоинство стеганографии перед криптографическими методами защиты информации заключается в том, что обеспечивается скрытие самого факта существования конфиденциальных сведений при их передаче, хранении или обработке. Для стеганографии наиболее интересно с практической точки зрения использовать текстовую информацию и изображения [1].

В настоящее время в качестве стеганоалгоритмов применяется метод замены наименее значимого бита. Суть данного метода заключается в том, что наименее значимые биты цифрового изображения или аудиофайла могут быть заменены данными из текстового файла таким образом, что посторонний независимый наблюдатель не обнаружит никакой потери в качестве изображения или звука.

С массовой компьютеризацией всех сфер деятельности человека объем информации, хранимой в электронном виде, возрос в тысячи раз. Это, в свою очередь, значительно повысило риск утечки информации. В связи с этим возникает задача увеличения объёма информации, встраиваемой в стеганограмму [2].

В данной работе для решения сформулированной задачи предлагается использовать метод скрытия информации в неподвижных изображениях, предусматривающий замену не одного, а двух наименее значимых бит. Использование предлагаемого метода позволяет увеличить вдвое количество информации, встраиваемой в исходный файл, без потери визуального качества изображения. При этом были оценены основные характеристики стеганоалгоритмов, такие, как:

нормированная средняя абсолютная разность:

$$NAD = \sum_{x,y} \left| C_{x,y} - S_{x,y} \right| \Big/ \sum_{x,y} \left| C_{x,y} \right| , \qquad (1)$$

качество изображения:

$$IF = 1 - \sum_{x,y} (C_{x,y} - S_{x,y})^2 \Big/ \sum_{x,y} (C_{x,y})^2 . \qquad (2)$$

В представленных соотношениях через $C_{x,y}$ обозначается пиксель пустого контейнера с координатами (x, y), а через $S_{x,y}$ – соответствующий пиксель заполненного контейнера.

При этом данные показатели практически не изменяются по сравнению с методом замены одного наименее значимого бита.

В работе выполнен сравнительный анализ характеристик предлагаемого стеганоалгоритма и существующих методов скрытия информации в неподвижных изображениях. Результаты показали перспективность предлагаемого метода.

Литература: 1. Грибунин В. Г. Компьютерная стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев, В. Ю. Головачев, А. В. Коняев – М.: Солон-Р, 2002. – 272 с. 2. Аграновский А. В. Основы компьютеной стеганографии: Учеб. пособие для вузов / А. В. Аграновский, П. Н. Девянин, Р. А. Хади, А. В. Черемушкин. – М.: Радио и связь, 2003. – 151 с. // http://www.book.ru/74754 3. An Information-Theoretic Model for Steganography. Christian Cachin. Cambridge, 1998 // http://www.simovits.com/archive/stego.pdf.

Чєвардін В. Є.

Сорокін І. А.

УДК 2343.234

АНАЛІЗ ОСОБЛИВОСТЕЙ ІНФРАСТРУКТУР ВІДКРИТИХ КЛЮЧІВ

Одним із найважливіших питань у сучасних телекомунікаційних мережах є їх криптографічний захист і забезпечення її автентичності [1]. Підтвердженням цього є офіційні повідомлення про підробку сертифікатів навіть таких поважних компаній, як Microsoft. Інша причина обговорення зазначеної теми − наявність випадків, у яких неможливо отримати сертифікат або перевірити його істинність. Метою даної роботи є аналіз існуючих інфраструктур відкритих ключів (ІВК) [2; 3], їх переваг і недоліків та аналіз підходів до побудови ІВК в Україні.

Основними видами загроз для таких важливих автоматизованих систем, як банківські, ринкові або білінгові, є порушення їх афтентичності та цілісності під час різноманітних електронних

транзакцій. Для захисту від цих загроз широко використовують механізм електронного цифрового підпису (ЕЦП) у сукупності з процедурами сертифікації відкритих ключів, причому основна увага зловмисників зосереджується на способах імітації та підміни останніх. Тому в результаті аналізу систем безпеки у сучасних автоматизованих системах було з'ясовано, що особливе місце в них посідають центри розподілу відкритих ключів, ефективність функціонування відносин довіри в яких має прямий вплив на функціонування системи безпеки в цілому.

ІВК – це технологія, що поєднує апаратні та програмні модулі, політики та процедури. Технічно ІВК становить топологію мережних зв'язків центрів сертифікації ключів (ЦСК), що використовуються для розповсюдження відкритих ключів шифрування та цифрового підпису [3; 4].

На даний час при проектуванні систем безпеки звертають увагу на такі конфігурації топологій ІВК [4]:

ієрархічна;
мережна;
браузерна;
"міст довіри".

Подальший розгляд видів топологій ІВК показав, що для різних випадків застосування властива як унікальна конфігурація зв'язків ЦСК, так і набір довірчих відносин між ЦСК. Таким чином, залежно від типу топології ІВК, вона володітиме певними вадами або перевагами. Саме ці особливості ІВК визначатимуть сферу її застосування. Результатом аналізу стала порівняльна таблиця оцінки безпеки всіх типів ІВК.

У ході роботи були розглянуті криптографічні інтерфейси Win32 CryptoAPI, що входить до операційних систем Microsoft та PGP фірми Phil's Pretty Good Software. Окрім базових криптографічних перетворень, ці пакети здатні виконувати цілий ряд функцій більш високого рівня – підтримку сертифікатів X.509, захист секретів DPAPI та ін [5].

У результаті проведеної оцінки безпеки зроблено висновок про необхідність побудови гібридної ІВК, яка б відповідала вимогам окремих інформаційних структур. Це дозолить знизити ризики несанкціонованого втручання в сегменти ІВК та одночасно підвищити ефективність її роботи. Складністю такої побудови буде узгодження політик ЦСК різних видів. У подальшому планується провести кількісну оцінку безпеки кожного виду ІВК та розробити рекомендації щодо використання криптографічних методів безпеки.

Література: 1. Щербаков А. Прикладная криптографія / А. Щербаков, А. Домашев. – М.: Издательско-торговый дом "Русская редакция", 2003. – 416 с. 2. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework // http://www.ietf.org/rfc/rfc3647.txt 3. Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile // http://www.ietf.org/rfc/rfc3279.txt 4. Каплаур П. В. Постановление Совета директоров национального банка республики Беларусь 19 октября 2006 г. № 281 "Об утверждении Концепции созадния банковской инфрастурктуры открытых ключей" // Банкаускі веснік. – 2006. – №30 (359). – 52 с. 5. Клименко Е. О применении криптографических средств ОС Windows для маскирования информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. – Вип.10.

УДК 004.056.5

Гросфельд Ю. А.

Зуєнко А. В.

ВИЗНАЧЕННЯ ОПТИМАЛЬНОСТІ МЕТОДІВ ЗАХИСТУ DNS-СЕРВЕРІВ

Електронний бізнес фактично неможливий без належного захисту. Інформаційна безпека є одним із найважливіших елементів систем електронного бізнесу й повинна забезпечуватися цілим набором методів і засобів. Слід пам'ятати, що інформаційні потоки захищені настільки, наскільки захищеним є найслабкіше місце в інформаційній системі [1].

Проаналізувавши основні загрози, які чекають компанію, що займається електронною комерцією, і пов'язані з ними втрати, визначимо найбільш небезпечні та ймовірні щодо застосування атаки на DNS-сервери [2]:

1. Протокол DNS базується на не досить захищених протоколах нижнього рівня (IP, TCP, UDP).

---

2. Ступінь захисту інформаційних ресурсів організації не може впливати на успіх проведення таких атак.

3. Атака може мати продовження у вигляді ланцюгової реакції, скомпрометувати інші DNS-сервери.

4. Більшість атак на DNS-сервери є тривіальними й не вимагають від зловмисника практично ніякої кваліфікації.

Основні завдання, що потребують вирішення [3]:

визначення основних критеріїв оцінки якості роботи DNS-сервера;

створення математичної моделі функціонування DNS-сервера;

аналіз загроз, а також імовірність їх застосування на базі статистичних даних компетентних організацій із захисту інформації;

моделювання загроз, а також методи захисту від них;

порівняльний аналіз методів захисту, а також їх вплив на ефективність роботи DNS-сервера;

визначення критеріїв ефективності методів захисту.

Після аналізу всіх існуючих методів захисту [4] постає завдання, наскільки той або інший метод є ефективний, а також наскільки він впливає на якість обслуговування сервера. Критерієм якості обслуговування будемо вважати пропускну здатність DNS-сервера, а також швидкість обробки DNS-запитів.

У результаті даної роботи розроблено модель атак на DNS-сервер, а також проаналізовано методи захисту від них. Також проводилось тестування щодо надійності та відмовостійкості при використанні різних атак і методів захисту.

Література: 1. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 616 с. 2. Мак-Клар С. Секреты хакеров. Безопасность сетей – готовые решения / С. Мак-Клар, Д. Скембрей, Д. Курц. – 4-е изд. – М.: Вильямс, 2004. – 656 с. 3. Медведовский И. Д. Атака на Internet / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – 3-е изд. – М.: ДМК, 2000. – 336 с. 4. Альбитц П. DNS и BIND / П. Альбитц, К. Ли. – СПб.: Символ-Плюс, 2002. – 696 с.

Ткачов А. М.

Король О. Г.

УДК 336.717:004.78

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ АУТЕНТИЧНОСТИ БАНКОВСКОЙ ИНФОРМАЦИИ В ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ

Развитие электронных платежных систем тесно связано с механизмами аутентификации и авторизации пользователей. Такая система относится к сложным многоуровневым системам, в которых передача информации требует контроля безопасности на каждом уровне [1; 2].

Обеспечение аутентичности и целостности передаваемых банковских данных является одной из важнейших задач, стоящих при обмене информации между банком и его клиентами, для их обеспечения наиболее эффективными являются криптографические методы.

Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом. Проведенные исследования угроз несанкционированного доступа к банковской информации в электронных платежных системах показали, что особое место при передачи информации между банком и клиентами занимают механизмы аутентичности и электронных цифровых подписей (ЭЦП), обеспечивающие взаимную аутентификацию абонентов, причастность к формированию и получению сообщения.

В работе рассматриваются основные алгоритмы построения ЭЦП. При этом электронная цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. Система ЭЦП включает две процедуры: 1) процедуру постановки подписи; 2) процедуру проверки подписи. В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи − открытый ключ отправителя. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа [1; 3].

При формировании ЭЦП отправитель вычисляет хэш-функцию h(M) подписываемого текста M, предназначенного для сжатия подписываемого документа M до нескольких десятков или сотен

бит (фиксированной длины). Вычисленное значение хэш-функции h(M) представляет собой один короткий блок информации m, характеризующий весь текст M в целом. Затем число m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЦП для данного текста M. При проверке ЦП получатель сообщения снова вычисляет хэш-функцию m = h(M) принятого по каналу текста M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции [1; 2].

Программной реализацией механизмов аутентичности являются программные средства криптографической защиты банковской информации, построенные на симметричных блочных алгоритмах шифрования (ГОСТ 28147-89, DES) в режиме CBC или CPB.

Недостатком данной реализации является невозможность построить безопасную однонаправленную хэш-функцию. Альтернативным вариантом безопасного построения хэш-функции является использование блока сообщения в качестве ключа (предыдущее хэш-значение − в качестве входа, а текущее хэш-значение − в качестве выхода). Длина блока определяется длиной ключа, а длина хэш-значения совпадает с длиной блока.

Особое место среди механизмов аутентичности информации занимают схемы аутентификации, построенные на различных криптографических алгоритмах и реализующих итерационные хэш-функции, предназначенные для выработки образа хэшируемого сообщения (текста), определения и доказательства его подлинности и принадлежности истинному владельцу (объекту).

В работе рассматривается классификация наиболее известных схем аутентификации в зависимости от стойкости к атакам и типу используемого математического аппарата, что позволяет разделить их на MDC-коды детектирования ошибок и MAC-коды подлинности информационных последовательностей. Проведенный анализ показал, что использование вычислительно стойких схем аутентичности на основе блочных шифров (ГОСТ, DES и др.) не позволяет обеспечить доказуемо стойкие схемы аутентификации. Схемы хэширования, построенные на основе модульной арифметики, имеют слабую криптографическую стойкость и не позволяют обеспечить требуемые значения аутентичности и целостности. Схемы аутентификации доказуемой стойкости обеспечивают требуемые показатели криптостойкости, но имеют существенный недостаток − медленную скорость преобразования данных.

Рассмотренный трафик обработки банковских данных в СЭП позволил сделать вывод, что основная доля времени обработки транзакции банковских данных приходится на формирование и проверку контрольных последовательностей (кодов аутентификации и цифровой подписи). При увеличении длины модуля RSA с 512 бит до рекомендуемых 1024 бит приведет к значительному увеличению времени формирования и проверки криптографической контрольной последовательности. Вместе с тем, дальнейшее развитие и увеличение криптоаналитических атак указывают на необходимость интегрированного подхода для обеспечения защиты передаваемой информации [4].

Перспективным направлением решения задач обеспечения требуемых показателей является разработка хэш-функций доказуемой стойкости, которая позволит повысить стойкость аутентификации при сравнительной вычислительной сложности криптопреобразований.

Литература: 1. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; [Под ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с. 2. Столлингс В. Криптография и защита сетей: принципы и практика: Пер. с англ. – 2-е изд. – М.: Изд. дом "Вильям", 2001. – 672 с. 3. Логинов А. А. Общие принципы функционирования электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества / А. А. Логинов, Н. С. Елхимов // Конфидент. – 1995.– №4. – С. 48 – 54. 4. Кузнецов А. А. Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях / А. А. Кузнецов, С. П. Евсеев, Б. П. Томашевский, Ю. И. Жмурко // Зб. наук. праць ХУ ПС. – 2007. – Вип. 2 (14). – С. 102 – 111.

УДК 004.056.5

Говоров А. О.

Нікуліщев Г. І.

МОДЕЛЬ АВТОМАТИЗОВАНОЇ СИСТЕМИ МАЛОГО ПІДПРИЄМСТВА, ЗАХИЩЕНОЇ ВІД ІНСАЙДЕРІВ

В сфері інформаційної безпеки найбільшу увагу організації приділяють, як правило, захисту від зовнішніх атак та конкурентної розвідки. З цієї причини майже всі кошти, що виділяються на забезпечення безпеки, спрямовуються на захист вразливих точок периметру мережі підприємства.

Ситуація, що склалася, знайшла відповідне відображення й на ринку продуктів інформаційної безпеки – останніми роками пропонується широкий спектр різних засобів захисту від вірусів, хробаків, троянських програм та інших загроз ззовні.

Проте поступово керівники підприємств починають усвідомлювати нову небезпеку. Вона надходить не від хакерів, спаму або випадкових вірусів, а від власних співробітників. Інсайдери знаходяться всередині самої організації та наділені цілком легальними повноваженнями, тому їм набагато простіше отримати доступ до необхідної інформації, ніж будь-якому зловмисникові ззовні. Відстежити випадки таких порушень політики безпеки теж набагато складніше, оскільки не відбувається несанкціонованого проникнення до автоматизованої системи. За статистикою останніх років до 30% порушень політики безпеки відбувається внаслідок зловживань службовим становищем і повноваженнями або халатного ставлення з боку працівників організації, і ще 30% порушень заподіюються колишніми працівниками підприємств [1].

Під автоматизованою системою малого підприємства автори розуміють комп'ютерну мережу, що складається з декількох автоматизованих робочих місць користувачів та комп'ютера адміністратора безпеки, який виконує функції сервера. До складу мережі також можуть входити комп'ютери керівників підприємства. Можливо також, що фунції адміністратора безпеки виконує один із керівників малого підприємства.

Найбільш вразливе для інсайдерів місце в такій системі – USB-порти, оскільки через них можна скопіювати інформацію на різні переносні пристрої: флеш-карти, мобільні телефони, фотоапарати, плеєри тощо. Також певну загрозу становлять пристрої читання CD- та DVD-дисків, що підтримують функцію запису. Комерційні продукти, покликані вирішити цю проблему, зазвичай становлять програмне забезпечення, яке надає можливість обмежувати й контролювати доступ до портів USBі дискових пристроїв. Вартість таких програм може досягати 500 у.о. [2].

Запропонована модель захищеної мережі малого підприємства передбачає замість використання програмних засобів розмежування доступу до USB портів і дискових пристроїв їхню фізичну відсутність. Авторами пропонується не обладнувати автоматизовані робочі місця користувачів системи пристроями читання дисків, а USB-порти відключати від материнської плати. Якщо фізичне відключення неможливе, відсутність доступу до портів пропонується забезбечити засобами BIOS, доступ до налаштувань якого має захищатися паролем [3].

Модель, запропонована авторами, передбачає наявність робочих портів USB і пристроїв читання CD та DVD дисків на машинах керівного складу та/або адміністратора безпеки. Таким чином, згідно з моделлю, запис інформації з мережі на зовнішні пристрої та її зчитування з них відбувається під контролем відповідальних осіб. Ризик витоку інформації описаним шляхом мінімізується.

У результаті запропонована модель дозволяє економити кошти підприємства, по-перше, на пристроях читання CD- та DVD-дисків і, по-друге, на програмному забезпеченні, яке використовується для розмежування доступу до цих пристроїв і портів USB. Надійність запропонованого методу забезпечується фізичним відключенням потенційно небезпечних пристроїв та портів.

Література: 1. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб.: Питер, 2008. – 320 с. 2. Соколов А. В Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. – М.:ДМК Пресс, – 2002. – 656 с. 3. Белунцов В. Настройка BIOS. Практическое руководство. – М.: Изд: ТехБук, 2004. – 400 с.

Долгов В. И.

Ивонин Д. С.

УДК 681.3.06: 519.248.681

КРИПТОАНАЛИЗ УМЕНЬШЕННОЙ МОДЕЛИ СИММЕТРИЧНОГО БЛОЧНОГО АЛГОРИТМА ШИФРОВАНИЯ NIMBUS

Алгоритм шифрования Nimbus, один из участников конкурса NESSIE, разработан Алексисом Уорнером Мачадо из компании Gauss Informatica, Бразилия. Данный шифр вызывает интерес тем, что он имеет достаточно высокое быстродействие и при этом является одним из самых простых алгоритмов [1].

Очевидно, что перед применением нового алгоритма шифрования, его следует тщательно протестировать и оценить стойкость к различным типам криптоаналитических атак, убедиться в том, что алгоритм не имеет слабых и/или эквивалентных ключей (или если они есть, то их количество не выходит за допустимые пределы).

Выполнить данную задачу для алгоритма, имеющего 64-битные блоки и 64-битные ключи (последние могут иметь длины до 576 бит), очень сложно и долго, даже имея в распоряжении целую сеть мощных компьютеров. Поэтому был применен метод, который заключается в криптоанализе уменьшенной модели алгоритма шифрования, а именно уменьшенного шифра с длиной блока и длиной ключа 16 бит.

Такая уменьшенная модель названа mini-Nimbus. Для этой модели можно полным перебором найти все слабые и эквивалентные ключи за непродолжительный период времени. Получив такую статистику можно попытаться оценить соответствующие показатели для большого шифра (конечно, если соблюдены условия "эквивалентности" модели и прототипа) [2; 3].

В роботе представляются результаты исследования шифра mini-Nimbus в отмеченном направлении. Показывается, что для этого шифра при зашифровании одного и того же текста существует множество эквивалентных ключей. Для подтверждения этих результатов выполняется эксперимент с поиском эквивалентных ключей для большого шифра. Делается вывод обобщающего характера о слабых криптографических показателях шифра Nimbus.

Литература: 1. Панасенко С. П. Алгоритмы шифрования – участники конкурса NESSIE. Ч. 1 // http://www.-ixbt.com/soft/nessie-part1.shtml. 2. Machado A. W. The Nimbus Cipher // http://www.cosic.esat.kuleuven.be. 3. Furman V. Differential Cryptanalysis of Nimbus // http://data.mf.grsu.by/Crypto/papers /2355/23550187.pdf

УДК 621.391

Носик А. М.

Качур Л. Н.

НЕДВОИЧНЫЕ ПСЕВДОСЛУЧАЙНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ С УЛУЧШЕННЫМИ АНСАМБЛЕВЫМИ И КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

Научно-техническая задача построения больших ансамблей дискретных сигналов математически сопряжена с поиском эффективных методов и алгоритмов формирования псевдослучайных последовательностей с улучшенными ансамблевыми и корреляционными свойствами [1 – 3]. В работах [4 – 6] предложен новый подход к построению больших ансамблей двоичных псевдослучайных последовательностей, основный на псевдослучайном перестановочном преобразовании кодовых слов двоичного блокового кода. В работе [7] проведены статистические исследования формируемых таким образом последовательностей, установлено, что по своим корреляционным свойствам они не уступают квазиортогональным дискретным сигналам и обладают улучшенными ансамблевыми свойствами.

В данном докладе приводятся результаты исследований недвоичных псевдослучайных последовательностей с улучшенными ансамблевыми и корреляционными свойствами. В основе предлагаемого метода лежит использование обобщенно-перестановочных преобразований кодовых слов недвоичных линейных блоковых кодов. Обобщенно-перестановочное преобразование вектора $a = \{a1, a2, \ldots, an\}$, $ai \in GF(q)$, задается $n \times n$-матрицей с элементами из GF(q), причем в каждой строке и в каждом столбце матрицы M только один ненулевой элемент из GF(q). Результирующий вектор $a' = \{a'1, a'2, \ldots, a'n\}$, $a'i \in GF(q)$ формируется как результат произведения: $a' = aM$. В качестве кода использован недвоичный регистровый код максимальной длины над полем из четырех элементов. Полученные результаты показали, что формируемые последовательности обладают улучшенными ансамблевыми и корреляционными характеристиками. Мощность формируемых ансамблей задается числом обобщенно-перестановочных матриц и мощностью используемого кода. Сложность реализации устройств формирования псевдослучайных последовательностей растет линейно от длины последовательности.

Перспективным направлением дальнейших исследований является разработка методов и алгоритмов формирования обобщенно-перестановочных матриц, статистические исследования синтезируемых последовательностей, выработка практических рекомендаций по применению предлагаемого подхода.

Литература: 1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с. 2. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Сов. Радио, 1985. – 384 с. 3. Стасев Ю. В. Применение сложных сигналов в командно-телеметрических радиолиниях / Ю. В. Стасев, И. Д. Горбенко, Б. И. Макаренко, А. В. Ивашкин, Д. Н. Воронов // Космічна наука і технологія. – 1997. – Т. 3. – №5/6. – С. 104 – 108. 4. Кузнецов А. А. Синтез ансамблей дискретных сигналов с использованием алгебраических методов помехоустойчивого кодирования / А. А. Кузнецов, А. М. Носик, С. Ю. Стасев // Збірник наукових праць ХВУ. – 2006. – Вип. 6 (12). – С. 96 – 98. 5. Стасев Ю. В. Формирование псевдослучайных последовательностей с улучшенными автокорреляционными свойствами / Ю. В. Стасев, А. А. Кузнецов, А. М. Носик // Кибернетика и системный анализ: Международный научно-теоретический журнал. – 2007. – №1. – С. 3 – 16. 6. Кузнецов А. А. Формування великих ансамблів дискретних сигналів з поліпшеними кореляційними властивостями / А. А. Кузнецов, А. М. Коваленко, О. В. Харченко, О. М. Носік // Системи озброєння і військова техніка. – 2007. – Вип. 1 (9). – С. 94 – 98. 7. Кузнецов А. А. Формирование псевдослучайных последовательностей на основе методов алгебраического кодирования / А. А. Кузнецов, А. М. Носик, А. Н. Коваленко // Вісник Сумського державного університету. Технічні науки. – 2007. – №1. – С. 129 – 143.

Kostyshyn S.

УДК 004.056:004.7

SECURITY AND PRIVACY ISSUES OF UBIQUITOUS COMPUTING IN THE OFFICE SETTING

Ubiquitous computing (ubicomp) has been an area of considerable scientific interest since 1991. An outline of it and related security issues can be found, for example, in [1]. A large number of publications and projects have focused on ubicomp technologies in the home setting. In contrast, this paper overviews its security and privacy implications at the workplace.

There are several security-related features that a modern office ubicomp environment could be reasonably expected to possess as opposed to home and mobile contexts:

1. A network constantly managed by professionals and, to some extent, governed by centralized security policies.

2. Permanent Internet connection and, as a result, availability of trusted third parties for the purposes of authentification.

3.High or critical business value of information stored and, more importantly, transferred.

4. "Guest" people and devices whose identity may be hard to establish.

Privacy concerns are stronger in the office setting. Traditionally, home and wearable ubicomp devices are assumed to collect a spectrum of private information for purposes ranging from deducing personal preferences to providing medical care. On the other hand, in "weak" ubicomp [2] that is more realistic for modern offices, a large part of such information is next to useless and is not supposed to be acquired in the first place. Yet, it could be inferred from routinely gathered data or retrieved secretly.

Traditionally, security of a system is understood as a complex of its three properties: confidentiality, integrity and availability. The nature of pervasive computing has important implications on each of these components, especially the two latter [3]. Ubiquitous computing devices are usually characterized by tighter constraints than conventional personal computers, specifically of computing power, memory size and battery life (if applicable). With regard to encryption these constraints mean that use of "expensive" public key cryptography (in particular encryption and verification operations) should be minimized in favor of computationally "cheaper" symmetric cryptography [3]. Some authors also argue that "the domination of asymmetric cryptography has, in part, been spurred by the need to implement identity authentication" [4, p. 90], and therefore question its merits in ubicomp where the identity authentication is of low, if any, practical value (see below).

Much debate is evolving around the entities that are to be authenticated. Creese et al. [4] argue

that the traditional identity authentication is unsuitable for ubicomp for at least two reasons: interactions take place between devices, for which it might be impossible to establish identities; even if verified, such an identity itself gives no confidence about the device's future proper behavior. They suggest instead of that individual attributes of devices (location, manufacturer, state, history etc.) are authenticated, provided that such attributes are "chosen to achieve assurance about which devices are the subject of interaction, and what these devices will do" [4, p. 85].

The assumption we made about constant availability of trusted third parties in office environment is important here as in that case existing authentication techniques may be used.

Any device that carries some ID or certificate can become a target of attack seeking to extract that information. The small size of ubicomp nodes facilitates their theft and covert replacement. This means that it's reasonable to make the devices tamper resistant so that the ultimate cost of retrieving information from them becomes disproportionately high.

Regarding availability, ubicomp introduces a type of denial of service attacks aiming to deplete a device's battery. In the office environment this threat's severity can be limited, though not eliminated, by powering the devices centrally where possible.

Also one cannot avoid the social implications of ubicomp. By the very nature, it has a potential of an ideal surveillance system [1], "a dream comes true for electronic stalkers and "big brothers" [5, p. 1]. The discussion of privacy issues of ambient intelligence have become commonplace in scientific circles, to the extent that its prevalence has attracted criticism [2, p. 410]. However, it is widely believed that the future of ubicomp market would ultimately depend on its ability to ensure privacy of its users.

Paper [6] describes three domains of privacy in ubicomp: technical, regulatory (including legal) and sociological. Nowdays, the problems best developed within the technical domain are those of location privacy and user anonymity. Interesting recent works in this area include [7], introducing an intuitive concept of "virtual walls", and [5], describing a hierarchical structure creating a "mist" to hide user identities and/or physical location from other users and the system itself.

From a different perspective, [8] presents a device for aiding in RFID tag management, including blocking unwanted reader-tag interactions by means of selective jamming. Being probably an acceptable solution for well-informed individuals, this requires on the person's part more than could be expected from a typical ubicomp target user.

Robinson et al. [1] maintain that the technology itself is not enough to ensure privacy, and rely on legislation for protecting it. There is a progress in the area of privacy regulation in different jurisdictions, primarily EU and USA.

Finally, a number of publications treat the problem of privacy from the social perspective. For example, [9] coins such terms as "digital territory" and "virtual residence". That approach is highly intuitive, but it lacks a technical foundation. As a result, it remains unclear how (and whether) the suggested concepts could be implemented technologically in ubicomp.

Security and privacy of ubicomp are combinations of technological, legal and social challenges. This paper has attempted to highlight a number of such problems as relevant to present-day office environments employing limited implementations of the ubicomp potential.

References: 1. Robinson P. Some Research Challenges in Pervasive Computing / P. Robinson, H. Vogt, W. Wagealla // Ed. P. Robinson, H. Vogt, W. Wagealla Privacy, Security and Trust within the Context of Pervasive Computing. – Springer, 2005. – P. 1 – 16. 2. Rogers. Y. Moving on from Weiser's Vision of Calm Computing: Engaging UbiComp Experiences // Ed. P. Dourish, A. Friday. Ubicomp 2006. – LNCS. Vol. 4206. – 2006. – P. 404 – 421. – http://www.slis.indiana.edu/faculty/yrogers/papers/Rogers_Ubicomp06.pdf. 3. Stajano F. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks/ F. Stajano, R. J. Anderson// 7th Security Protocols Workshop. LNCS. Vol. 1796. – Cambridge, 1999. – http://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf. 4. Creese S. Research Directions for Trust and Security in Human-Centric Computing / S. Creese, M. Goldsmith, B. Roscoe, I. Zakiuddin // Ed. P. Robinson, H. Vogt, W. Wagealla. Privacy, Security and Trust within the Context of Pervasive Computing. – Springer, 2005. – P. 83–91. 5. Al-Muhtadi J. Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments/ J. Al-Muhtadi, R. Campbell, A. Kapadia, M. Dennis Mickunas, S. Yi// International Conference of Distributed Computing Systems. – Vienna, 2002. – P. 65 – 74. – http://ciae.cs.uiuc.edu/mist/mist.pdf. 6. Gow G. Privacy and Ubiquitous Network Societies // ITU Workshop on Ubiquitous Network Societies. – ITU, 2005. – 34 p. – http://itu.int/spu/ni/ubiquitous. 7. Kapadia A. Virtual Walls: Protecting Digital Privacy in Pervasive Environments/ A. Kapadia, T. Henderson, J. J. Fielding, D. Kotz // International Conference on Pervasive Computing. – Springer, 2007. – 18 p. – http://www.ists.dartmouth. edu. 8. Rieback M. A Platform for RFID Security and Privacy Administration/ M. Rieback, G. Gaydadjiev, B. Crispo, R. Hofman, A. Tanenbaum. – 2006. – 14 p. – http://www.cs.vu.nl. 9. Daskala B. Digital Territories – Towards the protection of public and private space in a digital and Ambient Intelligence environment/ B. Daskala, I. Maghiros // Institute for Prospective Technological Studies (IPTS), 2007. – 122 p. – http://ftp.jrc.es /eur22765en.pdf .

Золотарьов В. А.

УДК 336.717

КРИТЕРІЇ ЗАХИЩЕНОСТІ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ВІД ВИТОКУ КАНАЛАМИ ПЕМВН

Виток інформації каналами побічних електромагнітних випромінювань і наводок (ПЕМВН) в телекомунікаційних мережах можливий як під час роботи обчислювальної техніки, так і в режимі очікування. Джерелами виникнення каналів ПЕМВН є: електромагнітні поля; електричний струм та напруга в провідних системах (живлення, заземлення та з'єднувальних); перевипромінювання інформації, що обробляється, на частотах паразитної генерації елементів і пристроїв технічних засобів обчислювальної техніки; перевипромінювання інформації, що обробляється, на частотах контрольно-вимірювальної апаратури.

Відповідно до середовища поширення інформаційних сигналів у телекомунікаційних мережах доцільно розглядати два можливих канали витоку. Перший − канали витоку за рахунок безпосередньо ПЕМВН; другий − комунікаційний канал витоку. За способом утворення розрізняють чотири типи каналів витоку в телекомунікаційних мережах.

Канал електромагнітного випромінювання (КЕМВ) [1]. Утворюється за рахунок полів, що виникають при проходженні інформації ланцюгами засобів обробки інформації (ЗОІ). КЕМВ характеризується розміром зони електромагнітного випромінювання − відстанню між ЗОІ та антеною апаратури перехоплення. Поза зоною практично неможливо ефективне приймання через природне зниження рівня сигналу, що випромінюється.

Канал випадкових антен (КВА). Виникає за рахунок наведеної ЕДС в струмопровідних комунікаціях, які гальванічно не пов'язані з ЗОІ та мають вихід за межі зони, що контролюється. КВА характеризується зонами для зосереджених випадкових антен (до яких відносять будь-які технічні засоби, що мають вихід за межі контрольованої зони) і розподільних випадкових антен (провід, кабель). Розмір зони випадкових антен визначається відстанню між ЗОІ та випадковими антенами, поза якими неможливе ефективне перехоплення інформаційного сигналу.

Канал комунікацій, що відходять від основної мережі та гальванічно зв'язаних із ЗОІ. Характеризується граничним припустимим значенням відношення потужності інформативного сигналу та нормованої завади, при якому неможливе ефективне приймання сигналу.

Канал нерівномірного споживання струму (КНСС). Утворюється за рахунок амплітудної модуляції струму спрацювання елементів ЗОІ під час обробки інформації [1]. Характеризується граничними припустимими значеннями відношення величини змінення струму, що надходить від джерела під час обробки інформації, до середньої величини струму споживання. Якщо зазначене відношення не перевищує граничного значення, то ефективне приймання по КНСС неможливе. Оскільки в сучасних засобах обчислювальної техніки практично відсутні низькошвидкісні пристрої (діапазон частот цього каналу приймається від 0 до 30 Гц), то цей канал витоку інформації вже не актуальний.

Таким чином можна сформулювати такий критерій захищеності ЗОІ від витоку через ПЕМВН. ЗОІ можна вважати захищеним, якщо: радіус зони електромагнітних випромінювань не перевищує мінімально припустимої відстані від ЗОІ до межі контрольованої зони; відношення потужностей інформативного сигналу нормованої завади в усіх випадкових антенах на межі контрольованої зони не перевищує граничної припустимої величини; відношення потужностей інформативного сигналу нормованої завади в усіх комунікаціях, що відходять, на межі контрольованої зони не перевищує гранично припустиму величину; відношення величини зміни струму "обробки" до середньої величини струму споживання від електричної мережі на межі контрольованої зони не перевищує гранично припустиме значення.

Література: 1. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. ТР ЕОТ – 95 // Збірка нормативних документів системи технічного захисту інформації. – К.: Державний комітет України з питань державних секретів та технічного захисту інформації, 1997. – С. 45 – 55. 2. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М.: Горячая линия – Телеком, 2005.

УДК 681.327

Лисенко І. В.

МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ НА ОСНОВІ ПРИНЦИПУ ДИВЕРСНОСТІ

Цілісність (і автентичність), разом з конфіденційністю, є найбільш важливою послугою (функцією) захисту даних, яка реалізується завдяки використанню ключових і безключових криптографічних функцій хешування (КФХ) [1]. Існуючі шляхи забезпечення (підвищення) цілісності і автентичності повідомлень спрямовані, перш за все, на ускладнення хешуючих криптоперетворень залежно від типу криптоаналізу, що використовується щодо конкретної КФХ (або деякого класу КФХ). Це стосується безключових КФХ (але не тільки) і частіше за все пов'язане зі збільшенням часу обчислення дайджесту повідомлення (або коду автентифікації повідомлення (КАП), якщо йдеться про ключові КХФ).

У зв'язку з цим, на погляд автора, для вирішення завдання підвищення цілісності повідомлень може бути використаний диверсний підхід, або принцип диверсності, який традиційно використовується для забезпечення гарантоздатності інформаційних та управляючих систем критичного застосування [2]. При цьому слід зазначити, що елементи диверсного підходу є присутніми під час виконання хешуючих криптоперетворень в деяких протоколах захисту інформації, що широко використовуються (наприклад, SSL і TLS) [1]. Відмінною рисою цього принципу є така організація криптосистеми, при якій згідно з деяким правилом є можливість застосовувати не тільки різні криптоалгоритми (криптопримітиви), але і їх параметри, структуру, режими використання.

У межах цього підходу запропоновано 3 моделі, при цьому перші дві орієнтовані на обчислення КАП, а третя – дайджест-повідомлення.

Так, модель 1 передбачає використання деякої множини криптоалгоритмів та режимів шифрування (що є відомими для криптоаналітика), з яких в кожному сеансі взаємодії між користувачами обираються конкретні криптоалгоритм і режим його використання (наприклад, Cipher Block Chaining (CBC) або Cipher FeedBack (CFB)) згідно з деяким правилом, застосування якого не дозволяє криптоаналітику одержати інформацію щодо того, які власне криптоалгоритм та режим його використання були використані під час обчислення КАП. При цьому це правило може бути як невідомим, так і відомим для криптоаналітика. В останньому випадку неоднозначність вибору параметрів криптосистеми забезпечується завдяки використанню таємного ключа обраного блокового симетричного криптоалгоритма [3].

Відмінність моделі 2 від моделі 1 полягає у тому, що в кожному сеансі використовуються різні криптоалгоритми для криптоперетворення різних блоків повідомлення на основі схеми CBC. При цьому правило вибору переметрів криптосистеми, що реалізується за рахунок звичайного модулярного перетворення, також може змінюваться від сеанса до сеанса, що, певна річ, передбачає існування правила вибору цього правила.

Таким чином, що стосується моделі 1, можна говорити про міжсеансову диверсність, а щодо моделі 2 – про внутішньосеансову диверсність.

Модель 3, також як і модель 2, реалізується в межах внутрішньосеансової диверсності [4]. Її сутність полягає у тому, що, по-перше, користувачі заздалегідь за допомогою деякого правила визначають перелік стандартних безключових КХФ (наприклад SHA-1, SHA-2 та ін.) із заданої їх множини $MH(\cdot) = \{H1(\cdot),\ldots,Hn(\cdot)\}$ для генерації дайджеста в даному сеансі. По-друге, в даній моделі використовується принцип композитності, згідно з яким здійснюється багатократне хешування повідомлення сумісно зі з'єднаним з ним дайджестом (ідея цього принципу базується на описаному в джерелі [5] підході, коли дайджест повідомлення є результатом конкатенації обчисленого його хеш-значення і хеш-значення, одержанного під час хеш-перетворення повідомлення зі з'єднаним попереднім хеш-значенням). Тобто типове хеш-перетворення у таком випадку визначається як раунд, і в загальному випадку користувачі виконують d раундів таким чином, що на кожному з них використовуються різні елементи множини $MH(\cdot)$. Формально результат хеш-перетворення на і-му раунді може бути представлений таким чином:

$mi = Hj(m0 \,||\, \ldots \,||\, mi\text{-}1 \,||\, M)$, $i = 1,\ldots,d$,

де $m0 = H(M)$ – дайджест повідомлення M, обчислений на першому раунді;

$||$ – оператор конкатенації.

Таким чином, результат хеш-перетворення на кожному раунді залежить від результатів хеш-перетворень на попередніх раундах.

Наприклад, якщо $|MH(\cdot)| = 2$, тобто використовуються дві різні КХФ $H1(\cdot)$ та $H2(\cdot)$, і $d = 2$, то можливими результатами обчислення дайджеста m повідомлення M відповідно до моделі 3 можуть бути:

$$m = m1 = H_1(M \,||\, m_0) = H_1(M \,||\, H_2(M));$$
$$m = m1 = H_2(M \,||\, m_0) = H_2(M \,||\, H_1(M));$$

$$m = m1 = H_1(M \,||\, m_0) = H_1(M \,||\, H_1(M));$$
$$m = m1 = H_2(M \,||\, m_0) = H_2(M \,||\, H_2(M)).$$

Два останніх співвідношення характеризують можливу ситуацію, коли одна й та ж хеш-функція використовується під час криптоперетворень на кожному з двох раундів. У загальному випадку, коли $|MH(\cdot)| = n$, якщо криптоперетворення здійснюються впродовж d раундів, усього можливо nd варіантів обчислення дайджесту, тобто ймовірність вгадати криптоаналітиком правильний варіант є 1/ nd.

Безсумнівно, що використання диверсного підходу потребує збільшення часу криптоперетворень (як для ключових, так і безключових КФХ), але це дозволить, як передбачається, підвищити криптостійкість механізму хешування за рахунок створення невизначеності для криптоаналітика щодо того, які алгоритми криптоперетворення були використані.

Література: 1. Столлингс В. Криптография и защита сетей. Принципы и практика. – К.: "Вильямс", 2001. – 668 с. 2. Харченко В. С. Гарантоспособность и гарантоспособные системы: элементы методологии// Радіоелектронні і комп'ютерні системи.– 2006. – Вип. 5(17). – С. 7 – 19. 3. Лысенко И. В. Модели обнаружения модификации сообщений с использованием симметричной криптографии на основе принципа диверсности / И. В. Лысенко, Т. А. Исиченко // Збірник наукових праць Харківського університету Повітряних Сил. – 2007. – Вип.1(13). – С. 70 – 72. 4. Лысенко И. В. Модель реализации криптографической функции хэширования на основе принципов диверсности и композитности // Радіоелектронні і комп'ютерні системи. – 2008. – Вип 7(34). – С. 84 – 86. 5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд. ТРИУМФ, 2003. – 816 с.

Коваленко А. Н.

Сай В. Н.

УДК 621.396

МЕТОД ФОРМИРОВАНИЯ АНСАМБЛЕЙ СЛОЖНЫХ СИГНАЛОВ С УЛУЧШЕННЫМИ СВОЙСТВАМИ ДЛЯ ПЕРСПЕКТИВНОЙ РАДИОСЕТИ УПРАВЛЕНИЯ

На современном этапе существования Вооруженных сил Украины актуальной проблемой есть принципиальное обновление вооружения и техники, в том числе создание перспективной радиосети управления [1].

Для обеспечения управления в условиях ведения боевых действий представляется предпочтительным применение широкополосных систем связи (высокая помехозащищенность, высокая пропускная способность, четкая передача данных в разговорном тракте, высокая энергетическая экономичность и экологичность терминального оборудования) [2; 3].

Качественные характеристики широкополосных систем связи в основном определяются ансамблевыми и корреляционными свойствами используемых ансамблей дискретных сигналов. Следовательно, актуальной научно-технической задачей есть разработка вычислительно эффективных методов формирования больших ансамблей дискретных сигналов с заданными значениями боковых выбросов функции корреляции.

На сегодняшний день практически все известные методы обладают рядом конструктивных недостатков, отсутствуют простые и вычислительно эффективные методы и алгоритмы формирования больших ансамблей сигналов с теоретически обоснованными значениями функции взаимной корреляции [2; 4]. Перспективным направлением в этом смысле является использование кодовых последовательностей циклических кодов, что позволяет формировать сигналы, имеющие хорошие автокорреляционные свойства [5]. В тоже время функция взаимной корреляции полученных дискретных сигналов имеет большие одиночные боковые выбросы, обусловленные цикличностью применяемого кода. Для решения этой задачи предлагается новый подход, основанный на выборке отдельных кодовых последовательностей не являющихся циклическим сдвигом друг друга. Это

позволяет получить множество псевдослучайных последовательностей с заданными корреляционными и ансамблевыми свойствами.

В работе теоретически обоснованы значения функций корреляции формируемых сигналов и приведен алгоритм построения ансамбля дискретных сигналов с заданными значениями боковых выбросов.

Литература: 1. Біла книга 2005: оборонна політика України. – К.: МО України, 2006. 2. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Сов. Радио, 1985. – 384 с. 3. Волков Л. Н. Системы цифровой радиосвязи: базовые методы и характеристики / Л. Н. Волков, М. С. Немировский, Ю. С. Шинаков. – М.: Эко-Трендз, 2005. – 392 с. 4. Свердлик М. Б. Оптимальные дискретные сигналы. – М.: Сов. Радио. – 1975. – 200 с. 5. Стасев Ю. В. Формирование псевдослучайных последовательностей с улучшенными автокорреляционными свойствами / Ю. В. Стасев, А. А. Кузнецов, А. М. Носик // Кибернетика и системный анализ. – 2007. – №1. – С. 3 – 16.

УДК 354.31(477)(004.7+65.012.8)

Кудінов В. А.

КОМПЛЕКСНИЙ ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ

В органах і підрозділах внутрішніх справ (ОВС), внутрішніх військах та навчальних закладах МВС України функціонує єдина система збирання, опрацювання та подання до Міністерства внутрішніх справ України, Головних управлінь МВС України в Автономній Республіці Крим, областях, містах Києві та Севастополі, на транспорті Головного управління внутрішніх військ МВС України оперативної інформації про резонансні злочини та інші надзвичайні події, що стались на території країни [1]. Метою функціонування цієї системи оперативного інформування (СОІ) МВС України є своєчасне реагування ОВС на надзвичайні ситуації, що виникають на території країни, стеження за розкриттям резонансних злочинів, своєчасне та якісне оперативне інформування керівництва МВС України, зацікавлених інстанцій, держави про стан оперативної обстановки в Україні для прийняття впливових управлінських рішень на її покращання.

СОІ МВС України становить організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Вона побудована у вигляді трирівневої ієрархічної моделі: 1) центральний рівень (підрозділ чергової частини (ЧЧ) Міністерства внутрішніх справ України); 2) обласний рівень (підрозділи ЧЧ головних управлінь (управлінь) МВС України в областях та на транспорті); 3) територіальний рівень (підрозділи ЧЧ міських, районних та лінійних ОВС). На кожному рівні в ЧЧ будуються локальні обчислювальні мережі, що об'єднують автоматизовані робочі місця (АРМ) працівників чергових частин і сервер з інформаційними обліками. Якщо розглянути АРМ працівників чергової частини центрального рівня, то воно включає в себе автоматизовану інформаційну систему "Зведення" (комплекс засобів обчислювальної техніки і спеціального програмного забезпечення, що дозволяє обробляти документи анкетного виду з формуванням баз даних реляційного типу), а також системи зв'язку телеграфними ("Телгком") і телефонними (електронна пошта) каналами [2]. Таким чином, сучасні інформаційні технології набули широкого застосування в практичній діяльності підрозділів чергових частин ОВС та забезпечують ефективне функціонування системи оперативного інформування МВС України. Але при цьому залишається не вирішеною проблема захисту оперативної інформації про резонансні злочини та інші надзвичайні події, що подається у вигляді спецповідомлень з територіального рівня СОІ МВС України до її обласного та центрального рівнів за відкритими каналами зв'язку. Відповідно до Постанови КМУ від 29.03.2006 № 373 [3] ця інформація підлягає захисту під час її обробки в системі.

Питанням аналізу загальної структури корпоративної мережі ОВС України, а також моделей об'єкта захисту інформації і можливого порушника безпеки мережі, присвячена стаття [4]. У роботах [5; 6] проведений аналіз проблем створення захисту конфіденційної інформації, що обробляється у системі оперативного інформування МВС України. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України, а також аналіз множини векторів-показників прояву загроз об'єктам захисту цієї інформаційної системи, наведений у статті [7]. У роботі [8] було розглянуто проблеми створення комплексної системи захисту корпоративної мережі ОВС України, а у роботі [9] досліджена проблема попередження комп'ютерних злочинів при передачі інформації в корпоративній мережі ОВС України.

Таким чином, враховуючи особливості обробки інформації в СОІ МВС України, необхідно здійснити належні заходи щодо її комплексного захисту, а саме, на кожному з трьох рівнів СОІ МВС України та під час передачі каналами зв'язку.

Література: 1. Наказ МВС України "Про вдосконалення реагування на повідомлення про злочини, інші правопорушення і події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України" від 04.10.2003 № 1155 // htpp: // www.nau.kiev.ua. 2. Кудинов В. А. Автоматизированное рабочее место дежурного дежурной части МВД-УМВД (УМВДТ) / В. А. Кудинов, Т. В. Рыбалко: Метод. рекомендации. – К.: РИО МВД Украины, 1996. – 100 с. 3. Постанова КМУ "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29 березня 2006 року № 373 // Урядовий кур'єр від 18.04.2006 № 73 // htpp: // www.kmu.gov.ua. 4. Хорошко В. О. Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки / В. О. Хорошко, В. А. Кудінов // Захист інформації. – 2004. – №1. – С. 26 – 35. 5. Кудінов В. А. Аналіз проблем створення захисту конфіденційної інформації, що обробляється в системі оперативного інформування МВС України // Сб. научн. тр. "Защита информации". –К.: НАУ, 2003. – С. 60 – 67. 6. Кудінов В. А. Проблеми захисту комп'ютерної інформації у процесі взаємодії чергових частин МВС-УМВС(УМВСТ) // Тр. Міжвуз. наук.-практ. конф. "Правові основи захисту комп'ютерної інформації від протиправних посягань" (22 грудня 2000 року). – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 187 – 190. 7. Хорошко В. О. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України / В. О. Хорошко, В. А. Кудінов // Захист інформації. – 2004. – № 4. – С. 11 – 18. 8. Хорошко В. О. Проблемы создания комплексной системы защиты корпоративной сети органов внутренних дел Украины/ В. О. Хорошко, В. А. Кудинов // Тр. XIII Междунар. научн. конф. "Информатизация и информационная безопасность правоохранительных органов" (25 – 26 мая 2004 г.). – М.: Академия управления МВД Росии, 2001. – С. 137 – 140. 9. Кудінов В. А. Проблема попередження комп'ютерних злочинів при передачі інформації в корпоративній мережі ОВС України // Злочини у сфері використання комп'ютерної техніки: проблеми кваліфікації, розслідування і попередження: Вісник ЛАВС МВС імені 10-річчя незалежності України. Спецвипуск. – Лу- ганськ: РВВ ЛАВС, 2005. – С. 48 – 51.

Щербаков А. В.

УДК 681.3.07

ИСПОЛЬЗОВАНИЕ МЕХАНИЗМОВ БЕЗОПАСНОСТИ В .NET

В настоящее время .NET становится основной платформой для разработки приложений [1; 2]. Одним из основных приоритетов в разработке приложений является безопасность. Грамотно организованная система безопасности приложения − это дополнительная гарантия сохранности и конфиденциальности данных, защита от несанкционированного доступа и многое другое [3]. Библиотека .NET Framework предоставляет для этого все необходимые средства.

Система безопасности в .NET состоит из нескольких служб, управление которыми доступно как администраторам, так и прикладным программистам. Основными из этих служб являются следующие: безопасность типов, аутентификация, авторизация, полномочия, политики безопасности, происхождение кода [3].

Безопасность типов играет одну из ключевых ролей − именно благодаря этому есть возможность изолировать сборки друг от друга, что дает возможность использовать в рамках одного процесса несколько сборок с разным уровнем доверия. Например, загрузив из Интернета безопасную сборку, можно быть уверенным, что она не вызовет WinAPI функцию, которая отформатирует жесткий диск. Также есть гарантия того, что безопасный код работает с другими объектами только дозволенным способом (например, не будет пытаться вызывать private-методы другого объекта). Само собой разумеется, что есть возможность отключить процесс проверки безопасности типов, однако, для того, чтобы это сделать, нужны достаточно серьезные полномочия.

Аутентификация представляет собой процесс проверки регистрационной информации пользователя [3]. Приложения в .NET Framework могут использовать большинство из доступных на настоящий момент механизмов аутентификации [1]. Примерами таких механизмов аутентификации являются Digest, Passport, аутентификация на основе служб предоставляемых операционной системой либо на основе механизмов, определенных в приложении. Управляемый код может получить регистрационную информацию и роли пользователя через объект Principal (интерфейс IPrincipal), который также содержит ссылку на Identity.

Авторизация − это процесс проверки прав текущего пользователя на выполнение запрошенного действия [3]. В процессе авторизации проверяется принадлежность пользователя к определенным ролям, и на основе этой информации принимается решение о предоставлении доступа к ресурсу.

В .NET Framework код может выполнить какое-либо действие только в том случае, если у него на это есть достаточно прав [1; 3]. Все это контролируется специальными объектами − Permissions. В свою очередь полномочия покрывают три области:

Code Access Permissions. Предоставляют доступ к защищенному ресурсу, либо возможность выполнить некую закрытую операцию;

Identity Permissions. Это группа характеристик, которые идентифицируют сборку. Common Language Runtime (CLR) создает эти полномочия на основе происхождения сборки. Identity permissions позволяют защитить код от неавторизированного доступа;

Role-based Permissions. Эта группа полномочий предоставляет механизм для проверки того, что вызывающий пользователь (либо агент, действующий от его имени) принадлежит к определенной роли.

Тут можно также отметить, что как полномочия, так и пользователи в .NET имеют мало общего с аналогичными сущностями в Windows. Как пример: права на доступ к файлу, лежащему на диске с NTFS, – пользователь, запустивший .NET приложение, может иметь соответствующие права на доступ в NTFS, но CLR все равно может не предоставить доступа к диску (если приложение запущено из сети), так и наоборот – CLR может разрешить действие с файлом, но ошибка проявится уже на уровне NTFS.

Политики безопасности представляют собой набор правил, на основе которых принимается решение о том, какие действия могут выполняться кодом, а какие нет. Каждый раз, когда загружается сборка, CLR проверяет ее происхождение и на основе этой информации и политики безопасности принимается решение о том, какие полномочия предоставить этой сборке.

В .NET Framework определено четыре группы политик [3]. Каждый из уровней содержит свой набор правил, на основе которых определяется, какие права можно предоставить коду.

Уровень Enterprise распространяется на каждый компьютер в домене и обычно управляется администраторами домена. По умолчанию на этом уровне всем сборкам (независимо от их происхождения) предоставляются полные права.

Уровень Machine распространяет свое действие на весь компьютер и может администрироваться локальным администратором или администратором домена. По умолчанию именно на этом уровне определяется большинство настроек безопасности.

Уровень Personal. Используется для управления настройками безопасности текущего пользователя. По умолчанию, как и на уровне Enterprise, всем сборкам даются полные права.

Уровень AppDomain. Это специальный уровень, и его настройки можно изменить только программно.

В момент загрузки кода происходит определение набора прав, которые предоставляются на каждом уровне, и после этого вычисляется минимальное множество прав, которое и будет ему гарантировано. И, если не менять никаких настроек, все реальные права определяются на уровне Machine (все остальные уровни предоставляют полный доступ).

Для назначения прав загруженному коду нужна информация о его происхождении. Происхождение кода и другая информация описывается специальным объектом Evidence [2; 3]. С точки зрения среды исполнения, объект Evidence – это коллекция идентификаторов, каждый из которых предоставляет разнообразную информацию о происхождении кода; она может быть двух видов: предоставленной тем, кто загружает сборку, или содержащейся внутри сборки.

Таким образом, использование механизмов безопасности при разработке приложений в .NET повышает надежность приложений и обеспечивает сохранность и конфиденциальность данных.

Литература: 1. Нейгел Кристиан. Ивьен и др. C# 2005 и платформа .NET 3.0 для профессионалов.: Пер. с англ. – М.: ООО "И.Д. Вильямс", 2008. – 1376 с. 2. Рихтер Дж. Программирование на платформе Microsoft .NET Framework / Пер. с англ. – 2-е изд., испр. – М.: Изд.-торг. дом "Русская редакция", 2003 – 512 с. 3. Казаков Тимофей. Механизмы безопасности в .NET // RSDN Magazine. – №4. – 2003 – С. 24 – 43.

УДК 004.056

Ziad S.

Malykhina T.

MAINTENANCE SAFETY IN OS LINUX

The purpose of the work is the comparative characteristic and the analysis of safety systems in some versions of OS Linux, as well as the studying of the questions connected with an increase of reliability of protection of system [1 – 4].

The brief overview of the references, is devoted to problems of safety in OS Linux. The analysis of the modern condition of the problem is presented in this report.

Some versions of Red Hat Linux and SUSE Linux 10.1 have been chosen for studying the problem of safety and priorities of protection [5 – 8]. The questions of the local security, the security of files and file system are presented in this work in detail. The report shows some of the additional means

---

given by Ext2 file system. In particular, recommendations on increase of reliability of a system protection, and safety of the user root are resulted.

Data encrypting algorithms and methods used in the various Linux versions are presented in this report for decision of the network safety questions.

This report also summarizes the currently available security features in typical Linux distributions, in addition to other security services and products that can be added. The authors also discuss ongoing research and development in future versions of Linux that will address emerging security requirements. In this report they focus on security requirements relevant to enterprise-level Internet servers. The authors show that current Linux distributions provide good security features, equivalent to other comparable operating systems. In addition, numerous optional services and products have been developed that provides further enterprise-level security functionality. The Linux community has also recognized the need for a single framework upon which this much of this functionality can be leveraged, called the Linux Security Modules (LSM). The authors should actively participate in making LSM a viable framework for meeting enterprise requirements and help the Linux community add further services to Linux to enable future systems to substantially reduce e-business security risks.

In the end of the report the authors say why they recommend to use Linux in business, science and other fields which use computers in work and studies.

References: 1. Петерсен Р. LINUX: руководство по операционной системе: В 2 т. Т. 1. – К.: Изд. группа BHV, 1998. – 528 с. 2. Петерсен. Р. LINUX: руководство по операционной системе: В 2 т. Т. 2. – К.: Изд. группа BHV, 1998.– 480 с. 3. Стахнов А. А. Linux. – СПб.: БХВ-Петербург, 2002. – 912 с. 4. http://www.linux-sec.net 5. Red Hat Linux 6.2: Учебн. курс / Под ред. А. Пасечкина. – СПб: Изд. "Питер", 2000. – 560 с. 6. Спесивцев А. В. Защита информации в персоналных ЭВМ/ А. В. Спесивцев, В. А. Вегнер, А. Ю. Крутяков и др. – М.: Радио и связь, МП "Веста", 1992. – 192 с. 7. http://seifried.org/lasg/filesystem/ 8. http://www.governmentsecurity.org /LinuxSecurity. php

Кузнецов А. А.

Грабчак В. И.

УДК 621.321

ДВОИЧНЫЕ ПСЕВДОСЛУЧАЙНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ С ТРЕХ- И ПЯТИУРОВНЕВОЙ ПЕРИОДИЧЕСКОЙ ФУНКЦИЕЙ КОРРЕЛЯЦИИ

Наибольшее распространение в современных системах цифровой связи нашли двоичные псевдослучайные последовательности: m-последовательности, последовательности Уолша, Голда, Кассами и др. [1 − 4]. Их периодические функции корреляции имеют n-уровневую структуру, определяемую свойствами порождающих многочленов [1; 2]. В работах [5; 6] исследованы вопросы синтеза двоичных псевдослучайных последовательностей с пятиуровневой функцией корреляции. Эти результаты с позиции единого общетеоретического подхода позволяют описать внутреннюю алгебраическую структуру синтезируемых последовательностей и обобщить некоторые известные методы на случай многоуровневой функции корреляции.

В данной работе авторами исследуются вопросы синтеза недвоичных псевдослучайных последовательностей с многоуровневой периодической функцией корреляции. Разрабатывается метод и практические алгоритмы формирования четверичных псевдослучайных последовательностей с трех- и пяти уровневой функцией корреляции. Исследуются ансамблевые свойства формируемых последовательностей, выводятся аналитические выражения, связывающие значения максимальных выбросов функции корреляции и мощность ансамбля формируемых последовательностей. При разработке метода формирования больших ансамблей сигналов использованы методы алгебраической теории блоковых кодов и комбинаторики. В терминах орбит линейный блоковый код описывается совокупностью непересекающихся множеств кодовых слов (орбит), причем каждая орбита содержит кодовое слово со всеми его циклическими сдвигами. Суть предлагаемого подхода состоит в формировании множества последовательностей как результат отбора по одному кодо-

вому слову из каждой орбиты. Результирующее множество содержит кодовые слова исходного кода, не являющиеся циклической сдвижкой друг друга. Дистанционные показатели кода гарантируют высокие корреляционные свойства ансамбля последовательностей, сформулированное правило отбора кодовых слов распространяет это свойство на любое значение сдвига при вычислении коэффициента корреляции периодических функций авто- и взаимной корреляции. Мощность формируемого ансамбля сигналов определяется как число орбит кода. Количество таких ансамблей определяется числом различных выборок кодовых слов из полного множества орбит кода. Перспективным направлением дальнейших исследований является разработка предложений по программной и аппаратной реализации предлагаемого метода, обоснование практических рекомендаций по его использованию в цифровых системах связи в том числе в системах связи с многостанционным доступом.

Литература: 1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с. 2. Гряник М. В. Технология CDMA – будущее сотовых систем в Украине / М. В. Гряник, В. И. Фролов // Мир связи. – 1998. – №3. – С. 40 – 43. 3. Свердлик М. Б. Оптимальные дискретные сигналы. – М.: Сов. Радио. – 1975. – 200 с. 4. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Сов. Радио, 1985. – 384 с. 5. Стасев Ю. В. Синтез дискретных сигналов с улучшенными свойствами / Ю. В. Стасев, А. А. Кузнецов, А. М. Носик, А. Н. Коваленко // Матеріали Третьої наукової конференції Харківського університету Повітряних Сил ім. Івана Кожедуба. – Харків: ХУПС, 2007. – С. 90. 6. Стасев Ю. В. Способ построения ансамблей дискретных сигналов с заданными значениями боковых выбросов корреляции / Ю. В. Стасев, А. А. Кузнецов, А. Н. Коваленко // Матеріали Першої науково-технічної конференції "Науково-методичні основи оцінювання та управління техногенною безпекою у разі виникнення надзвичайної ситуації" Програма конференції та тези доповідей. – Харків: НДІ мікрографії, 2007. – С. 7 – 8.

УДК 621.391

Пасько И. В.

Грабчак В. И.

ИССЛЕДОВАНИЕ ПОМЕХОУСТОЙЧИВОСТИ ПЕРЕДАЧИ ДИСКРЕТНЫХ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ

Эффективным средством повышения достоверности передачи данных в телекоммуникационных системах является помехоустойчивое кодирование [1 − 4]. Перспективным направлением его развития являются коды, возникающие на алгебраических кривых (алгеброгеометрические коды) [5 − 7]. Использование алгеброгеометрических кодов в каналах с независимыми и группирующимися ошибками позволяет получить энергетический выигрыш от кодирования и значительно снизить вероятность ошибочного приема дискретных сообщений [8; 9].

В то же время проведены исследования помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов построенных на плоских алгебраических кривых, заданных в проективном пространстве P^2 неприводимым однородным уравнением от трех переменных. Перспективным направлением дальнейших исследований является оценка помехоустойчивости передачи дискретных сообщений алгеброгеометрических кодов на пространственных кривых, задаваемых в пространстве P^3 совместными решениями совокупности двух однородных уравнений от четырех переменных.

В роботе автором излагаются основные научные и практические результаты, полученные в результате исследования помехоустойчивости передачи сообщений с использованием алгеброгеометрических кодов на пространственных кривых в дискретных каналах с независимым распределением ошибок [4;10]. Проведенные исследования показали, что применение алгеброгеометрических кодов на пространственных кривых позволяет существенно повысить помехоустойчивость передачи дискретных сообщений в каналах с независимым распределением ошибок. Асимптоти-

ческие свойства алгеброгеометрических кодов при увеличении длины кода и мощности алфавита символов обуславливают приближение к границе Шеннона вероятности ошибочного приема символов сообщения, что позволяет сделать вывод о высокой практической значимости полученных конструкций для повышения помехоустойчивости передачи дискретных сообщений.

Литература: 1. Берлекэмп Э. Р. Алгебраическая теория кодирования: Пер. с англ. – М.: Мир, 1971. – 478 с. 2. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с. 3. Злотник Б. М. Помехоустойчивые коды в системах связи. – М.: Радио и связь, 1989. – 232 с. 4. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с. 5. Гоппа В. Д. Коды на алгебраических кривых // Докл. АН СССР, 1981. – Т.259. – №6. – С. 1289 – 1290. 6. Кузнецов А. А. Алгеброгеометрические коды на пространственных кривых / А. А. Кузнецов, И. В. Пасько // Матеріали Першої науково-технічної конференції "Науково-методичні основи оцінювання та управління техногенною безпекою у разі виникнення надзвичайної ситуації". Програма конференції та тези доповідей. – Харків: НДІ макрографії, 2007. – С. 8 – 9. 7. Науменко М. І. Теоретичні основи побудови алгебраїчних кодів. Монографія / М. І. Науменко, Ю. В. Стасєв, О. О. Кузнецов. – Харків: ХУПС, 2005. – 268 с. 8. Кузнецов А. А. Энергетический выигрыш алгеброгеометрического кодирования// Радиотехника. – 2003. – Вып.134. – С. 218 – 222. 9. Кузнецов А. А. Энергетическая эффективность алгеброгеометрических кодов // Электронное моделирование. – 2004. – №2. – С. 27 – 38. 10. Бондарев В. Н. Цифровая обработка сигналов/ В. Н. Бондарев, Г. Трестер. – Харьков: Б.и., 2001. – 400 с

Королев Р. В.

Томашевский Б. П.

МЕТОД ФОРМИРОВАНИЯ НЕДВОИЧНЫХ РАВНОВЕСНЫХ ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Методы и алгоритмы формирования равновесных двоичных последовательностей широко применяются в помехоустойчивом кодировании для обнаружения ошибок в дискретных несимметричных каналах [1; 2], а также в крипто-кодовых схемах защиты информации как основной узел формирования сеансовых (разовых) ключей [3; 4]. В работах [5; 6] исследованы крипто-кодовые схемы, построенные по недвоичным блоковым кодам, в том числе по кодам Рида-Соломона, алгеброгеометрическим кодам и др. Установлено, что наиболее перспективными по соотношению криптографическая стойкость/ вычислительная сложность крипто-кодовых преобразований являются длинные недвоичные коды, построенные по алгебраическим кривым с малым значением отношения рода кривой к числу точек. В то же время отсутствие регулярных алгоритмов формирования недвоичных равновесных дискретных последовательностей сдерживает дальнейшее развитие крипто-кодовых средств защиты информации на недвоичных кодах. Актуальность разработки эффективных методов формирования недвоичных равновесных дискретных последовательностей обусловлена также необходимостью решения важной научно-прикладной задачи обнаружения сложных комбинаций ошибок в недвоичных дискретных несимметричных каналах.

В работе авторами представлены результаты исследований методов и алгоритмов формирования недвоичных равновесных дискретных последовательностей. Использованные методы исследований (комбинаторики, теории чисел и полей Галуа) позволили формализовать постановку задачи и получить ее аналитическое решение. Впервые разработан метод недвоичного равновесного кодирования, который основан на комбинированном биномиально-позиционном представлении чисел и позволяет, в отличие от известных методов двоичного равновесного кодирования, формировать дискретные последовательности с элементами из произвольного недвоичного числового поля с фиксированным весом Хемминга (фиксированным числом ненулевых элементов последовательности). В результате проведенных исследований предложены вычислительный алгоритм формирования недвоичных равновесных дискретных последовательностей и структурная схема соответствующего устройства, для программной и аппаратной реализации предложенного методов. Разработана имитационная модель устройства, проведены экспериментальные исследования, результаты которых подтверждают достоверность полученных результатов.

Перспективным направлением дальнейших исследований является разработка криптокодовых средств защиты информации с устройством формирования недвоичных равновесных дискретных последовательностей в качестве узла формирования сеансовых (разовых) ключей, исследование эффективных процедур обнаружения сложных комбинаций ошибок в недвоичных дискретных несимметричных каналах с использованием предложенных равновесных кодовых конструкций.

Литература: 1. Мак-Вильямс Ф. Дж. Теория кодов исправляющих ошибки. – М.: Связь 1979. – 744 с. 2. Влэдуц С. Г. Алгеброгеометрические коды.Основные понятия / С. Г. Влэдуц, Д. Ю. Ногин. – М.:МЦНМО, 2003. – 504 с. 3. Борисенко А. А. Нумерация равновесных кодов на основе биномиальных чисел //Вісник Сумського державного університету. – 1994. – №2. – С. 74-77. 4. Лидл Р. Конечные поля: В 2-х т.Т.1 / Р. Лидл, Г. Нидеррайтер: Пер.с анг. – М.:Мир,1988. – 430 с. 5. Сидельников В. М. Криптография и теория кодирования, 2002. – 22 с // http://ru.dleex.com/books. 6. Кузнецов А. А. Несимметричные криптосистемы на алгеброгеометрических кодах //Системи обробки інформації. – 2005 – Вип.1(41). – С. 210 – 216. 7. Кузнецов А. А. Исследование свойств несимметричных теоретико-кодовых схем с эллиптическими кодами / А. А. Кузнецов, В. Н. Лысенко, С. П. Евсеев // Системи обробки інформації. – 2004. – Вып. 9(37). – С. 79 – 84.

УДК 681.3.06: 519.248.681

Халімов Г. З.

Сєвєрінов О. В.

АНАЛІЗ МЕТОДІВ АВТЕНТИФІКАЦІЇ БАГАТОАДРЕСНОГО ДЖЕРЕЛА ДАНИХ

Багатоадресна передача є додатком, орієнтованим на групове обслуговування користувачів. Застосування традиційних методів криптографії для забезпечення автентифікації джерела даних при багатоадресній передачі не є ефективним. Неприйнятність звичних механізмів обумовлена багатобічним характером додатків і типом даних, які складаються, звичайно, з безперервного потоку багатоадресних повідомлень з передачею їх в реальному масштабі часу.

Протоколи автентифікації багатоадресного джерела даних поділяються на три категорії:

протоколи з використанням асиметрії секретної інформації групи користувачів, що розділяється між членами;

протоколи з використанням часової асиметрії при розподіленні секретної інформації між членами групи користувачів;

протоколи на основі гібридних схем асиметрії секретної інформації та часової асиметрії.

Протокол Desmedt, Frankel, Yung [1] з використанням асиметрії секретної інформації між членами групи користувачів будується на основі поліноміальної схеми. Джерело генерує поліном AM(x) ступеня k для повідомлення M. Кожному одержувачу надсилається розділений поліном. Щоб підроблювати автентифікатор повідомлення, необхідно мати не менше k частин полінома для його відновлення. Оскільки найбільше об'єднання шахрайських одержувачів може мати тільки k-1 членів, тим самим забезпечується безпека системи. Протокол допускає втрату пакету, оскільки кожен пакет містить свою автентифікаційну інформацію і, отже, може бути перевірений незалежно від інших пакетів.

Canetti та ін. [2] розглянули протокол, сутність якого полягає у тому, що відправник додає до кожного багатоадресного повідомлення M, l MAC кодів, використовуючи l різних ключів. Кожен одержувач володіє підмножиною ключів з числа l ключів відправника і перевіряє достовірність одержаних повідомлень, використовуючи свою підмножину ключів. Для супротивника, щоб підроблювати повідомлення правильного відправника, необхідно заволодіти l ключами з об'єднання w одержувачів.

У протоколах з використанням часової асиметрії цієї категорії обмежується час життя ключів, що використовуються для автентифікації багатоадресних пакетів. Перший протокол даної категорії запропонований Bergadano та ін. [2]. Сутність протоколу полягає в автентифікації кожного пакету даних за допомогою MAC при використанні ключа, який генерується на основі односторонніх ланцюжків. Щоб шахрайські одержувачі не використовували одержаний ключ для підробки пакетів даних від імені легітимного відправника, відправник гарантує, що ключі будуть відомі одержувачам, тільки коли всі одержувачі одержать пакети. Протокол Bergadano мінімізує розмір автентифікаційної інформації до одного MAC на пакет даних. Допускається втрата пакету також як і втрата ключа. Синхронізація одержувачів з часом відправника залишається головним недоліком методу.

Широкомовний автентифікаційний протокол TESLA був запропонований групою авторів Perrig та ін. [3]. Головна ідея TESLA полягає в тому, що відправник використовує різні ключі в кожен проміжок часу для автентифікації багатоадресних повідомлень в цей проміжок часу. TESLA ви-

користовує одноразові ключові ланцюги для генерації MAC ключів. Секретний MAC ключ зберігається відправником у секреті, щоб уникнути отримання ключа атакуючим, до того, як його отримав правильні одержувачі.

Perrig [3] запропонував протокол гібридної асиметрії, використовуючи нову одноразову сигнатурну схему, яка називається BiBa (Bins і Balls). Методологія підпису BiBa ґрунтується на принципово новому підході: використовуванні ефекту колізій.

У протоколі BiBa допускається втрата пакетів, оскільки кожен пакет супроводжується разом зі своїм BiBa підписом незалежно від інших пакетів. BiBa не уразливий до змов зловмисних одержувачів, оскільки відправник задіює новий набір ключів після кожного проміжку часу.

Більшість із протоколів, які забезпечують автентифікацію багатоадресного джерела даних, допускає втрату пакетів, тому що кожен пакет несе в собі свою власну автентифікаційну інформацію, незалежно від інших пакетів.

TESLA і рішення, запропоновані Bergadano та іншими, страждають від того, що одержувачі повинні буферизувати одержані пакети до тих пір, поки відповідний ключ верифікації не відкритий відправником. Інше рішення − це протокол, запропонований Canetti та іншими, автентифікація і верифікація в якому обмежується тільки моментом MAC обчислень (без затримок). Проте це рішення може використовуватися тільки у середовищах, де коаліція певної кількості шахрайських користувачів неможлива. У протоколі BiBa автентифікаційна інформація генерується і перевіряється негайно (без очікування іншої інформації) і вона нечутлива до коаліцій. Проте процес генерації автентифікаційної інформації відносно повільний (порівняно з рішенням Canetti та ін.).

Протокол BiBa і поліноміальна схема Desmedt та інші не є відповідним рішенням для середовищ з обмеженими ресурсами. Кращими протоколами за вимогами обчислювальної потужності є TESLA і рішення, запропоноване Bergadano, та ін. Проте ці два протоколи вимагають буферизувати пакети, одержані в певний проміжок часу.

Найкращим запропонованим рішенням з пропускної спроможності є протоколи TESLA і Bergadano та ін. Їх витрати на пропускну спроможність зменшуються до одного MAC (порядка 128 біт, використовуючи MD5) на доповнення до відкриття одного ключа за проміжок часу.

Література: 1. Fiat M. Naor, Broadcast encryption, "Advances in Cryptology-CRYPTO '93", Lecture Notes in Computer Science773 (1994). – P. 480 – 491. 2. Luby M. Combinatorial bounds for broadcast encryption / M. Luby, J. Staddon // Advances in Cryptology-EUROCRYPT'98, LNCS 1403, K. Nyberg, Ed. Espoo, Finland: Springer-Verlag, 1998. 3. Wong C. K. Secure group communications using key graphs / C. K.Wong, M. Gouda, S.S. Lam // IEEE/ACM Trans. Networking – Feb. 2000. – Vol. 8 – P. 16 – 30.

Сергиенко Р. В.

Белоковаленко А. Л.

УДК 681.3.06

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ ADE И AES С ИСПОЛЬЗОВАНИЕМ ИХ МИНИ-ВЕРСИЙ

В настоящее время в Украине проходит открытый конкурс по выдвижению и отбору кандидатов на национальный стандарт блочного симметричного шифрования. Одним из основных требований, предъявляемых к алгоритмам-кандидатам, была выдвинута высокая криптографическая стойкость к известным видам атак, также было рекомендовано учитывать опыт прошедших конкурсов криптоалгоритмов AES и NESSIE [1]. Несомненным фаворитом этих конкурсов являлся алгоритм Rijndael, который после победы в конкурсе AES стал известен как национальный алгоритм шифрования США AES − Advanced Encryption Standard [2; 3]. Высокие результаты этого алгоритма побудили многих криптографов мира как к криптоанализу данного алгоритма, так и к различного рода улучшениям его в свете выявленных потенциальных слабостей, порожденных простотой его алгебраической структуры.

Одним из возможных таких модернизаций является алгоритм криптографических преобразований информации с динамически управляемыми криптопримитивами, названный ADE (Algorithm of Dynamic Encryption), который является кандидатом на национальный алгоритм шифрования Украины [1; 2]. Основной задачей, которую поставили перед собой конструкторы этого шифра, является снижение потенциальной уязвимости шифра AES к атакам, которые могут использовать простоту алгебраического описания шифра [2], не допуская в то же время снижение стойкости к "классическим" статистическим атакам.

По мнению многих отечественных и зарубежных криптографов, дополнительное повышение показателей стойкости шифра может быть достигнуто на основе введения в шифрующие преобразования механизмов динамического управления промежуточными состояниями [2]. Создание на этапе формирования раундовых ключей блоков замен и матриц линейного рассеивания в зависимости от значений этих ключей позволяет получить дополнительное повышение сложности (размерности) системы алгебраических уравнений, описывающих процедуру зашифрования, не затрагивая принципиальной основы использованных в AES решений [2]. С целью проверки данного предположения были проведены исследования дифференциальных свойств мини-версий шифров AES и ADE, а именно таблиц распределения полных дифференциалов мини-шифров mini-AES и baby-ADE. Принципы создания этой масштабной модели во многом повторяют принципы, по которым создана одна из наиболее удачных мини-версий шифра AES – mini-AES, описание которого было опубликовано в открытой печати [4]. По результатам сравнения характеристик мини-шифров mini-AES и baby-ADE сделано заключение о сравнимости характеристик шифров-прототипов: AES и ADE.

В результате проведенных экспериментальных исследований установлено, что мини-шифр baby-ADE обладает лучшими свойствами, чем mini-AES, что подтверждает теоретические данные о повышении стойкости шифров вследствие введения ключезависимости в криптопримитивы раундовой функции. На основе этого сделан вывод, что ADE имеет, по меньшей мере, не худшие дифференциальные свойства, чем шифр AES.

Литература: 1. http://dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=49027&cat_id=38710 2. Кузнецов А. А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / А. А. Кузнецов, Р. В. Сергиенко, А. А. Наумко Радиотехника. – 2007. – Вып. 2. – С. 241 – 249. 3. http://portal.acm.org/citation.cfm?id=1278177.1278185&coll=&dl=&tyty=series&idx=SERIES418&part=series&WantType=Proceedings&title=ISSAI/ Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag. 4. https://www.cosic.esat. kuleuven.be/index.html/ Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students, Cryptologia, XXVI (4), 2002. L. R. Knudsen, "The number of rounds in block ciphers." Public report, NESSIE, 2000.

УДК 621.327

Лосєв М. Ю.

Федорченко В. М.

АНАЛІЗ ЕФЕКТИВНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Управління передачею інформації шляхом регулювання доступу до всіх ресурсів технічних, організаційних або програмних систем є одним із найважливіших напрямів сучасної фінансової або економічної діяльності людини. При цьому регламентуються порядок роботи користувачів і персоналу, право доступу до певної інформації або окремих файлів.

Вибір способів передачі інформації в комп'ютерних системах – складне інформаційне завдання, при вирішенні якого доводиться враховувати ефективність використання різних протоколів обміну даними, вірогідність виникнення помилок в інформаційних пакетах, вірогідність загроз, вартість реалізації різних способів захисту, модель порушника.

При глобальному керуванні навантаженням (доступом у мережу передачі даних) можна регулювати загальну кількість пакетів, що перебувають на обслуговуванні в телекомунікаційній системи. Для здійснення такого управління необхідно повідомляти відправника про доставку пакета. У вигляді таких повідомлень можуть виступати сигнали дозволу на передачу пакета. При цьому пакети виділяються в мережу тільки після одержання такого сигналу. Усього ж кількість дозволяючих сигналів у мережі цілком визначена. У кожному вузлі комутації у спеціальному пристрої повинно зберігатися визначена кількість дозволів. Після видачі пакета з мережі видаються дозволи для передачі нового пакета.

Слід зазначити, що міжвузлове управління не захищає від перевантаження, а управління доступом у мережу – від блокування. Метою наскрізного управління (від входу в мережу до виходу з неї) є узгодження швидкостей видачі пакетів у мережу і видачі їх з мережі, що забезпечує мінімум часу затримки пакетів і усуває блокування у вхідному вузлі, якщо потрібно проводити упорядкування та збирання повідомлень [1].

Основними операціями наскрізного управління є активізація логічних з'єднань, організація повторних передач і обмеження навантаження на логічне з'єднання. Процес активізації включає запит відправника про можливість прийому пакетів одержувачем і обмін різними службовими пакетами. Організація повторних передач при наскрізному керуванні необхідна для усунення помилок, що виникають на вузлах комутації. Помилки, що виникають у каналах телекомунікаційній системи, усуваються за рахунок повторних передач [2].

Сьогодні майже виключне розповсюдження знайшли методи підвищення достовірності передачі інформації з використанням зворотного зв'язку між користувачами телекомунікаційної системи. Введення зворотного зв'язку дає можливість шляхом проведення постійного аналізу помилок встановлювати фактичний стан каналів телекомунікаційної системи під час передачі та вводити надлишок, що дозволяє досягнути потрібної достовірності.

За видом зворотного зв'язку розрізняють системи з інформаційним, вирішальним та комбінованим зворотним зв'язком.

Перевагою систем з інформаційним зворотним зв'язком є їх порівняно проста реалізація, особливо при пробудові низькошвидкісних систем предачі даних, а суттєвим недоліком, який обмежує їх застосування, є висока завантаженість зворотного каналу передачею ретранслюваного потоку інформації [2]. Тільки тому в АСУ найбільш широко застосовуються системи з вирішальним зворотним зв'язком (ВЗЗ).

У системах з ВЗЗ повідомлення, що передаються, кодуються завадостійким кодом, який забезпечує виявлення помилок. Приймач, прийнявши повідомлення, виділяє пакети, котрі містять помилки, і посилає зворотним каналом сигнал перезапиту (вирішальний сигнал), у результаті чого проводиться повторна передача інформації.

Проведені дослідження показали, що системи з ВЗЗ, що використовують канали вивлення помилок, ефективніше систем без зворотного зв'язку, котрі використовують коди з виправленням помилок.

Література: 1. Лосев М. Ю. А.С. №1608815 СССР МКИ G06F13/00 // Бюлетень. – 15.06.92. – №22. – 8 с. 2. Лосев М. Ю. А.С. №1795459 СССР МКИ G06F11/00 // Бюлетень. – 15.02.93. – №6. – 4 с.

Чєвардін В. Є.

Чекурда О. М.

УДК 621.322

ПРОГРАМНИЙ КОМПЛЕКС ФОРМУВАННЯ КОДІВ АВТЕНТИФІКАЦІЇ ПОВІДОМЛЕНЬ ДЛЯ ПІДВИЩЕННЯ ІМІТОСТІЙКОСТІ ДАНИХ

Актуальність даної роботи полягає у необхідності дослідження засобів забезпечення імітостійкості даних у спеціальних телекомунікаційних системах (ТКС), прикладом яких є військові ТКС (Дніпро, Крапати, Ореанда та ін.). У зв'язку з розвитком нових методів обчислення великих масивів даних виникає необхідність підвищення вимог до існуючих методів імітозахисту даних і вдосконалення технічних засобів засекречування каналів зв'язку.

Важливість цього питання полягає в тому, що зараз відбувається широке втілення інформаційних технологій у ЗСУ, а саме – створення і впровадження телекомунікаційних систем і мереж, які дозволяють вирішувати різні завдання набагато продуктивніше.

Забезпечення імітостійкісті у ТКС військового призначення слід розглядати як забезпечення автентифікації.

У даному випадку маються на увазі ТКС військового призначення, що побудовані за допомогою сучасного обладнання: комутатор А-101, маршрутизатор А-202, ЦАКС-2, модем М-101, радіошлюз Р-126 та інші.

Зразки апаратури, що забезпечують безпеку інформації, і перебувають на озброєнні в ЗС України застарілі і потребують модернізації. Зокрема більшість хоча і забезпечують високу стійкість, але не пристосовані для роботи з цифровими каналами, що є обов'язковою вимогою до апаратури сучасних ТКС, або працюють з досить малими швидкостями. Нещодавно прийнято на озброєння апаратуру криптографічного захисту інформації "Пелена", яка відповідає вимогам до сучасної спецапаратури. Але "Пелена" здійснює засекречування саме каналу зв'язку, а не самого повідомлення. Це не забезпечує максимального рівня безпеки інформації [1].

Сучасні засоби засекречування повинні мати досить високу стійкість і швидкість роботи. Стійкість в основному залежить від розміру ключа та блоку шифрування. У теперішніх умовах розвитку обчислювальної техніки (суперкомп'ютерів) довжина ключа повинна бути не менше 60 біт, щоб забезпечити досить високу стійкість алгоритму засекречування [2; 3].

Для забезпечення автентифікації найбільш розповсюдженими є два засоби: електронний цифровий підпис і коди автентифікації повідомлень (MAC). Другий засіб особливо підходить при передачі великої кількості малих повідомлень за якомога короткий проміжок часу, що є особливо актуальним у ТКС військового призначення [1; 4].

Саме тому об'єктом дослідження було обрано MAC-коди.

При проведенні досліджень були отримані наступні результати:

1. Проведено аналіз існуючих засобів забезпечення автентифікації в ТКС [2; 3].

2. Розроблено програмну реалізацію алгоритмів формування MAC-кодів повідомлень в середовищі програмування C++ Builder.

3. За допомогою пакету статистичних тестів NIST проведено тестування хеш-послідовностей, утворених з використанням розробленого програмного додатку.

4. Проведена оцінка стійкості алгоритму і розроблено рекомендації щодо її підвищення.

Література: 1. Поповский В. В. Защита информации в телекоммуникационных системах Учебник / В. В. Поповский, Ф. В. Персиков. – Харьков: ООО "Компания СМИТ", 2006 – Т.1 – 292 с. 2. Иванов М. Л. Криптография. Криптографические методы защиты информации в комп'ютерных системах и сетях. – М: "Кудиц-образ", 2001. – 368 с. 3. Молдован А. Л. Криптография. Скоростные шифры. – СПб: "БХВ-Петербург", 2002. – 496 с. 4. Апрановский Ф. В. Практическая криптография, алгоритмы и их применение / Ф. В. Апрановский, Р. Хади. – М.: Салон-Пресс, 2002. – 256 с. 5. Домашев А. В. Программирование алгоритмов защиты информации. Учебное пособие. – М.: Издательство "Нолидж", 2002. – 416 с.

УДК 681.3.06

Шарапов В. Г.

ТЕСТУВАННЯ ВИПАДКОВИХ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ З ВИКОРИСТАННЯМ КОНТЕКСТНОГО МОДЕЛЮВАННЯ

Серед множини різних тестів перевірки якості випадкових і псевдовипадкових послідовностей особливу групу становлять тести, засновані на стисненні інформації [1]. Через те, що в існуючих тестах, побудованих за таким принципом, використовуються лише окремі методи стиснення [2], пропонується випробувати інші методи стиснення для побудови тестів, які аналізують властивості випадковості послідовностей.

На сьогоднішній день одними з найефективніших алгоритмів стиснення інформації є методи контекстного моделювання [1]. Унаслідок чого метод контекстного стиснення взято за основу для побудови способу тестування двійкових послідовностей на випадковість.

Сутність алгоритму полягає у тому, що, переглядаючи якийсь рядок зліва направо, можна на основі вже переглянутої частини робити певні прогнози щодо решти символів.

Перед кожним символом рядка, окрім першого, є інші символи − контекст. Коли зустрічається якийсь символ, то він зустрічається у якомусь контексті. Тобто, коли ми знову побачимо цей контекст, то ми зможемо спрогнозувати певний символ. Ідея алгоритму полягає в тому, що по черзі переглядаючи символи рядка, зліва направо, ми оновлюємо контексти і прогнозуємо такі символи. При цьому можна помилятись у символі, що прогнозується. Кількість правильних прогнозів входить до чисельних характеристик алгоритму.

При реалізації алгоритму необхідно враховувати такі правила:

задається найбільший контекст, контексти більшого порядку, ніж встановлений, не розглядаються;

перед символом переглядаються контексти, починаючи від максимального (або найбільш можливого для даного символу) до найменшого − нульового (пустого);

прогноз виконується за контекстами, які вже зустрічалися раніше і за якими одиниці та нулі були у різній кількості;

якщо за якимось контекстом прогнозується символ, то символ буде або передбаченим, або непередбаченим;

символ буде непередбачуваним, якщо за жодним контекстом, що йому передує, неможливо зробити прогноз;

результатом роботи алгоритму є кількість правильно/неправильно передбачених символів та кількість непередбачуваних символів.

Критерій оцінки якості послідовності за таким алгоритмом полягає у тому, що перевіряються кількісні характеристики, отримані алгоритмом, до відповідності теоретичному (експериментальному) розподіленню, що відповідає довжині вхідної послідовності.

За допомогою емпіричних випробувань було встановлено, що:

алгоритм ефективно відрізняє "цілком випадкові" послідовності від послідовностей, що певним чином відрізняються від таких;

алгоритм можливо застосовувати для послідовностей з довжиною 48 біт та більше;

алгоритм надає можливість відрізняти характеристики різних відхилень від "цілком випадкової" послідовності, а також ідентифікувати деякі типи генераторів;

алгоритм дає можливість відрізняти змістовні тексти (на будь-якій мові) від випадкових послідовностей, а також допомагає визначити мову тексту.

Основними перевагами даного алгоритму є те, що він ефективний навіть для дуже коротких послідовностей та надає чисельний результат для будь-яких вхідних даних, незалежно від їх випадковості.

Література: 1. Ватолин Д. Методы сжатия данных. Устройства архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ–МИФИ, 2003. – 384 с. 2. Тесты NIST и их описание // http://www.csrc.nist.gov/rng/. 3. Шарапов В. Г. Алгоритм тестування випадкових та псевдовипадкових послідовностей з використанням контекстного моделювання // Збірник тез доповідей учасників V Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених "Технології безпеки інформації" (19 квітня 2007 р., м. Київ). – К.: Б. в., 2007. – С. 24 – 25.

Shcherbakov O.

УДК 681.3.07

CODE ACCESS SECURITY IN .NET

Code access security is a feature of .NET that manages code, dependent on our level of trust [1]. If the Common Language Runtime (CLR) trusts the code enough to allow it to run, it will begin executing the code. Depending on the permissions provided to the assembly, however, it might run within a restricted environment. If the code is not trusted enough to run, or if it runs but then attempts to perform an action, for which it does not have the relevant permissions, a security exception (of type Security Exception, or a subclass of it) is thrown. The code access security system means that we can stop malicious code running, but we can also allow code to run within a protected environment where we are confident that it cannot do any damage.

For example, if a user attempted to run an application that attempted to execute code downloaded from the Internet, the default security policy would raise an exception and the application would fail to start [2]. In a similar way, if the user ran an application from a network drive it would begin executing, but if the application then attempted to access a file on the local drive, the runtime would raise an exception and, depending on the error handling in the application, would either gracefully degrade or exit.

For most applications, .NET's code access security is a significant benefit, but one that sits at the back of the room quietly helping out. It provides high levels of protection from malicious code, but generally, you do not need to get involved. However, one area you will be involved in is the management of security policy, and this is especially true when configuring desktops to trust code from the locations of software suppliers who are delivering applications to you [1; 3].

Another area, where code access security is a very important aspect is when you are building an application that includes an element whose security you want to control closely. For example, if there is a database within your organization containing extremely sensitive data, you would use code access security to state what code is allowed to access that database, and what code must not access it.

It is important to realize how code access security is about protecting resources (local drive, network, user interface) from malicious code; it is not primarily a tool for protecting software from users.

For security in relation to users, you will generally use the built-in Windows user security subsystem, or make use of .NET role-based security, which we discuss later in this chapter.

Code access security is based on two high-level concepts: code groups and permissions [1].

Code groups bring together code with similar characteristics, although the most important property is usually where the code came from. Two examples for code groups are Internet and Intranet. The group Internet defines code that is sourced from the Internet, the group Intranet defines code sourced from the LAN. The information used to place assemblies into code groups is called evidence. Other evidence is collected by the CLR, including the publisher of the code, the strong name, and (where applicable) the URI from which it was downloaded. Code groups are arranged in a hierarchy, and assemblies are nearly always matched to several code groups.

The code group at the root of the hierarchy is called All Code and contains all other code groups. The hierarchy is used for deciding which code groups an assembly belongs to; if an assembly does not provide evidence that matches it to a group in the tree, no attempt is made to match it to code groups below.

Permissions are the actions we allow each code group to perform. For example, permissions include “able to access the user interface” and “able to access local storage.” The system administrator usually manages the permissions at the enterprise, machine, and user levels.

The Virtual Execution System (VES) within the CLR loads and runs programs. It provides the functionality required to execute managed code and uses assembly metadata to connect modules together at run time [1].

When the VES loads an assembly, the VES matches the assembly to one or more of a number of code groups. Each code group is assigned to one or more permissions that specify what actions assemblies can do in that code group. For example, if the MyComputer code group is assigned the permission FileIOPermission, this means that assemblies from the local machine can read and write to the local file system.

References: 1. Robinson Simon. Professional C# / Simon Robinson, Christian Nagel, Jay Glynn, Morgan Skinner, Karli Watson, Bill Evjen. – Third Edition. − Wiley Publishing, Inc., 2006 – 1326 p. 2. Шилдг Герберт. Полный справочник по C#: Пер. с англ. – М. : Изд. дом "Вильямс", 2004. – 752 с. 3. Троелсен. Э. C# и платформа .NET. Библиотека программиста. – СПб.: Питер, 2004. –796 с.

УДК 004.056.57:656.2

Приходько С. И.

Безверхая Г. С.

КОМПЛЕКСИРОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ

Комплексирование механизмов защиты − это ключевой вопрос обеспечения информационной безопасности. Недостаточность либо некорректность исполнения механизмов приводит к уязвимости защиты, избыточность − к дополнительным затратам: затратам вычислительных ресурсов и финансовым затратам потребителя. Это определяет многокритериальную оптимизационную задачу и, в зависимости от того, какой критерий выбран доминирующим, получается принципиально различающиеся решения. Таким образом, предлагается рассматривать комплексирование механизмов защиты как многокритериальную оптимизационную задачу [1].

Пусть имеется определенное количество вариантов действий − количество угроз в системе. Исходя из литературных источников [2 − 4], можно выделить и проранжировать следующие источники угроз:

Искусственные угрозы (Λ_1):

1.1. Непреднамеренные (N_1) − это действия, которые совершают люди по неосторожности, незнанию, невнимательности или из любопытства. К такому типу угроз относят установку программных продуктов, которые не входят в список необходимых для работы, и в последствии могут стать причиной нестабильной работы системы и потери информации. Сюда же можно отнести и другие действия, которые не являлись злым умыслом, а люди, совершавшие их, не осознавали по-

следствий. Этот вид угроз трудно поддается контролю, важно чтобы персонал был квалифицирован, чтобы каждый человек осознавал риск, который возникает при его несанкционированных действиях.

1.2. Преднамеренные (N_2) – угрозы, связанные со злым умыслом преднамеренного физического разрушения, впоследствии выхода из строя системы. К преднамеренным угрозам относятся внутренние и внешние атаки.

1.2.1. Внутренние (N_1^2) – те действия, которые осуществляются через внутреннюю сеть, к этим угрозам относятся как угрозы технического характера $(N_1^2)_T$ (получение доступа к засекреченной информации путем взлома паролей, незаконная авторизация либо идентификация и т. д.), так и организационного $(N_1^2)_O$ (прямое либо косвенное воздействие на персонал).

1.2.2. Внешние (N_2^2) – те действия, которые совершаются за пределами сети предприятия, например, удаленный доступ через Интернет.

Естественные угрозы (Λ_2) – пожары, наводнения, удары молний, ураганы и другие стихийные бедствия, которые не зависят от человека.

Опираясь на вышеизложенную классификацию угроз можно определить, что количество вариантов воздействия на систему информационной безопасности M является:

$$M = \Lambda_1 + \Lambda_2 = (N_1 + N_2) + \Lambda_2 = \left\langle N_1 + \left\{ [(N_1^2)_T + (N_1^2)_O] + N_2^2 \right\} \right\rangle + \Lambda_2 = (1 + (2+1)) + 1 = 5 .$$

Было бы неправильно только посчитать варианты воздействий на систему ИБ, так как каждая угроза имеет свою степень опасности, необходимо дополнительно проранжировать источники угроз.

При выборе метода ранжирования источников угроз использовалась методология, изложенная в международных стандартах [4], и опыт российских экспертов в области информационной безопасности.

В качестве критериев сравнения (показателей) можно, к примеру, выбрать [3]:

I. Возможность возникновения источника $(K^1)i$ – определяет степень доступности к защищаемому объекту, удаленность от защищаемого объекта или особенности обстановки.

II. Готовность источника $(K^2)i$ – определяет степень квалификации и привлекательность совершения деяний со стороны источника угрозы, или наличие необходимых условий.

III. Фатальность $(K^3)i$ – определяет степень неустранимости последствий реализации угрозы.

Если учесть, что вышеприведенные показатели могут принимать значения от 1 до 5 [3], то число вариантов атак (Y) в системе можно вычислить по формуле:

$$Y = K^1 \cdot K^2 \cdot K^3 \cdot M = \left((C_5^1)^3 \right)_i \cdot M = \left(\frac{5!}{1!(5-1)!} \right)^3 \cdot 5 = 625 .$$

То есть количество вариантов атак, как и количество вариантов защиты, равно 625.

Таким образом, комплексирование механизмов защиты – это выбор оптимальной стратегии защиты информации из множества многокритериальных вариантов. Следовательно, сформулирована многокритериальная оптимизационная задача. Данную задачу можно рассмотреть как сражение двух противников: первый – защитник, задача которого построить систему защиты так, чтобы атака была нереализуема, и второй – злоумышленник, задача которого удачно атаковать систему защиты. Из этого следует, что в такой постановке данную многокритериальную многопараметрическую задачу лучше всего решать с помощью применения теории игр.

Литература: 1. Щеглов А. Ю. Общие вопросы построения системы защиты информации / А. Ю. Щеглов, К. А. Щеглов // http://articles.security-bridge.com/articles/91/11670. 2. Игнатенко С. А. ГОСТ Р ИСО/МЭК 15408-2002: спустя три года // http://www.itsec.ru/articles2/pravo/ gost_p_iso_mek_15408. 3. Вихорев С. В. Классификация угроз информационной безопасности // «Сетевые атаки и системы информационной безопасности 2001» // http://Cnews.ru. 4. Угрозы информационной безопасности // http://www.infobezpeka.com/publications /?id=91. 5. Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 "Практические правила управления информационной безопасностью"). 6. Руководящий документ "Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации" // Сборник руководящих документов по защите информации от несанкционированного доступа. – М.: Гостехкомиссия России, 1998. – С. 4.

УДК 519.711/.72

Белецкий А. Я.

ОБОБЩЕННЫЕ ПРЕОБРАЗОВАНИЯ ГРЕЯ. ТЕОРИЯ И ПРАКТИКА

Коды Грея, предложенные в середине XX века в ответ на запросы инженерной практики относительно построения оптимальных по критерию минимума ошибки неоднозначности преобразователей типа “угол–код”, на заре своего появления привлекли к себе внимание не только исследователей математиков, но и широкий круг разработчиков разнообразной аппаратуры. Отличительная особенность кодов Грея состоит в том, что в двоичном пространстве (или в двоичной системе счисления) при переходе от изображения одного числа к изображению соседнего старшего или соседнего младшего числа происходит изменение цифр (1 на 0 или наоборот) только в одном разряде числа.

За пятидесятилетнюю историю своего развития теория кодов Грея претерпела незначительные изменения. По-видимому, оказались вне поля зрения как математиков, так и разработчиков аппаратуры возможности построения кодов, инверсных по направлению формирования классическим кодам Грея. В известной схеме процесс формирования прямых и обратных кодов Грея развивается слева направо. Вместе с тем можно построить схему преобразования m-х кодов, обратную по направлению классическому (левостороннему) преобразованию Грея. В таком классе преобразований, который назван правосторонним, при прямом и обратном преобразованиях сохраняется неизменным значение младшего (правого) разряда преобразуемого числа.

Комбинация лево- и правостороннего преобразования по Грею (как прямого, так и обратного) совместно с операцией инверсной перестановки послужила основой построения комбинированных или составных кодов Грея. Применение составных кодов оказалось весьма успешным в задачах определения структуры и взаимосвязи базисных симметрических систем Виленкина–Крестенсона функций (ВКФ), частным случаем которых являются системы функций Уолша. И, тем не менее, не для всех порядков систем ВКФ удается □связать□полное множество систем. Возникает так называемая проблема кластеризации, которая, для примера, проявляется в том, что только 126 из 448 систем функций Уолша 16-го порядка оказалось возможным синтезировать с помощью простых кодов Грея. Обозначенную проблему кластеризации удалось разрешить введением обобщенных кодов Грея [1].

В работе рассматриваются различные направления применения разрабатываемых обобщенных преобразований Грея: в криптографии, теории и практике построения перестановочных счетчиков Грея и др. [2].

Литература: 1. Белецкий А. Я. Обобщенные преобразования Грея // Кибернетика и вычисл. техника. – 2004. – Вып. 145. – С. 58 – 77. 2. Белецкий А. Я. Основы теории. В 2-х т. / А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий Т.1. – К.: Кн. изд. НАУ, 2007. – 412 с. 3. Белецкий А. Я. Прикладные аспекты. Т.2. / А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий – К.: Кн. изд. НАУ, 2007. – 644 с.

УДК 681.3.06

Московченко И. В.

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ С ПОМОЩЬЮ МЕТОДА ГРАДИЕНТНОГО СПУСКА

В настоящее время обеспечение безопасности информации в информационно-телекоммуникационных системах является одной из первоочередных задач. Данная задача, в частности, может быть решена за счет использования симметричных схем криптопреобразования, стойкость которых обеспечивается за счет использования нелинейных преобразований. Поэтому разработка нелинейных преобразований, обеспечивающих стойкость к современным методам криптоанализа, является актуальной задачей.

В качестве нелинейных преобразований в симметричных криптосистемах используются нелинейные булевы функции [1 – 6]. Разработка таких функций является областью широких исследований. В статье [1] авторами представлен метод построения нелинейных булевых функций, основанный на градиентном спуске. В качестве прототипа разработанного метода формирования булевых функций использовался метод градиентного подъема [2], который является на сегодняшний день одним из наиболее эффективных методов формирования криптографических булевых функций. Оба метода относятся к классу эвристических методов и потенциально позволяют достигать бо́льших показателей стойкости. В данной статье исследуются криптографические свойства функций, построенных в соответствии с источником [1].

При проведении исследований криптографических свойств нелинейных булевых функций использованы следующие показатели: сбалансированность, нелинейность N_f, алгебраическая степень *deg*, значение функции автокорреляции *ac*, степень корреляционного иммунитета *CI*, степень критерия распространения *PC*. Методика исследования и детальное описание данных показателей представлены в статье [3]. При описании основных показателей использованы следующие типы формализованной записи [4]:

(*n, deg,* N_f*, ac*) – если не обсуждаются показатели *CI* и *PC*;

(*n, CI/PC, deg,* N_f*, ac*) – если данные показатели обсуждаются;

где *n* – размерность функции.

В качестве дополнительных показателей рассмотрены также: коэффициент равномерности минимизации корреляции $k_{рм}$ и абсолютное значение корреляции функции C_f [3].

В табл. 1 приведены сравнительные характеристики основных показателей стойкости функций, полученных с использованием разработанного и наилучших известных эвристических методов.

Таблица 1

Наилучшие известные профили (*n*, *deg*(*f*), N_f, *AC*)

NLT [4]	(5,3,12,8) (5,4,12,16)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24) (8,5,112,16)
	(9,8,238,40)	(10,9,486,72) (10,9,484,64)	(11,9,984,96) (11,10,982,96)	(12,10,1992,156) (12,10,1990,144)
ACT [4]	(5,3,12,8) (5,4,12,16)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24) (8,5,112,16)
	(9,8,238,40)	(10,9,484,56)	(11,10,982,88)	(12,11,1986,128)
Разработанный метод	-	(6,5,26,8)	-	(8,7,116,16)
	-	(10,8,488,32)	-	(12,11,1998,72)

Как видно из приведенной таблицы, разработанный метод позволяет строить функции с наилучшими известными на сегодняшний день профилями. Так, на сегодняшний день функции, построенные над V_6, имели наилучший профиль (6,5,26,16), теперь данный профиль имеет вид (6,5,26,8) (значение функции автокорреляции уменьшено в 2 раза); функции, построенные над V_8, имели наилучший профиль (8,7,116,24), теперь данный профиль имеет вид (8,7,116,16) (значение функции автокорреляции уменьшено в 1,5 раза); функции, построенные над V_{10}, имели наилучший профиль (10, 9, 484, 56), теперь данный профиль имеет вид (10, 8, 488, 32) (значение функции автокорреляции уменьшено в 1,75 раза); функции, построенные над V_{12}, имели наилучший профиль (12, 10, 1992, 156), теперь данный профиль имеет вид (12, 11, 1998, 72) (значение функции автокорреляции уменьшено в 2,16 раза).

В табл. 2 представлены дополнительные показатели стойкости, характеризующие спектральные свойства бент-функций, функций, построенных в соответствии с предлагаемым и известными алгебраическими и эвристическими методами построения высоконелинейных булевых функций.

Таблица 2

Дополнительные показатели стойкости нелинейных булевых функций

	N_f	*deg(f)*	$k_{рм}$	C_f
Бент-функция [4]	120	4	1	0,06250
Разработанный метод	116	7	1,058333	0,09375
Метод Кларка [4]	116	6	1.099567	0,09375
Метод Маитры–Пасалика [7]	116	6	1.154545	0,09375
Метод Себерри–Чжаня (*КИ*)	112	4	1.322917	0,12500

Приведенные данные показывают, что булевые функции, построенные в соответствии с разработанным методом, при равных наивысших показателях нелинейности с другими функциями имеют максимально достижимую алгебраическую степень, при этом все остальные известные методы уступают по своим спектральным характеристикам.

Литература: 1. Кузнецов А. А. Метод построения криптографически стойких булевых функций на основе градиентного спуска / А. А. Кузнецов, Ю. А. Избенко, И. В. Московченко // Зб. наук. пр. ХУ ПС. – Харків: ХУПС. – 2007. – Вип. 1 (13). – С. 63 − 66. 2. Millan W. "Smart Hill Climbing Finds Better Boolean Functions" / W. Millan, A. Clark and E. Dawson // Workshop on Selected Areas in Cryptograph. − 1997 (SAC'97). − P. 50. 3. Горбенко И. Д. Исследование аналитических и статистических свойств булевых функций криптоалгоритма Rijndael (FIPS 197)/ И. Д. Горбенко, А. В. Потий, Ю. А. Избенко // Радиотехника. − 2004. − № 126. − С. 132 − 138. 4. Clark J. Evolving of Boolean functions satisfying multiple criteria/ J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan // Proceedings of INDOCRYPT'02, LNCS. − 2002. − Vol 2551. − P. 246–259. 5. Maier W. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology / W. Maier, O. Staffelbach // EUROCRYPT'89. Lecture Notes in Computer Science. − 1990. − Vol. 434. − P. 549−562. 6. Millan W. An effective genetic algorithm for finding highly nonlinear Boolean functions/ W. Millan, A. Clark and E. Dawson // First International Conference on Information and Communications Security // Lecture Notes in Computer Science. − 1997.− №1334. − P. 149–158.

УДК 004.056

Белодед Н. И.

Рыбина Т. А.

БЕЗОПАСНОСТЬ WEB-СЕРВЕРОВ

В современных условиях развития ИКТ необходимо обеспечение защиты данных различными путями. Защищая сервер, администратор не всегда задумывается о том, как будет работать эта защита, а ведь именно от этого зависит безопасность информации[1 − 6]. Интернет уже давно перестал быть просто сетью из html-страниц. Сегодня это еще и сложные приложения, скрипты, транспортные сети, телеконференции, электронная почта и многое другое, значит и система безопасности сервера также должна становиться более сложной и совершенной.

Основными причинами растущей уязвимости информационных систем сегодня являются: регулярная смена конфигурации сетей (особенно характерно для развивающихся организаций); большое число лиц, имеющих root или администраторский доступ к серверу; использование как пиратского, так и лицензионного программного обеспечения (ПО) и др [1; 2; 4; 7]. Из вышеизложенного очевидно, что защита сервера сводиться к управлению рисками.

Сегодня иерархию защиты делят на шесть уровней. На первом уровне главный инструмент защиты − firewall. Второй уровень подразумевает конфигурацию ОС, под управлением которой работает сервер. Третий уровень − защита сети, оснащение датчиками атаки сетевого оборудования и ПО провайдера. Четвертый уровень − установка ПО на уровне хостинга (на этом уровне, как правило, возникает множество проблем). Пятый уровень принято делить на два подуровня: А и В. На уровне А устанавливается специальное ПО, которое играет роль прослойки между ОС сервера и всеми приложениями; на уровне В устанавливается ориентированные на конкретные приложения firewall и/или прокси-серверы. Шестой уровень − своеобразная вершина безопасности. Этот уровень предполагает использование ОС и приложений, разработанных специально для данной компании.

Уровень защиты сервера необходимо выбирать исходя из потребностей и финансовых возможностей организации [3]. Однако существуют и общие, наиболее простые правила, которые необходимо соблюдать для обеспечения безопасности. Так, например, размещение сервера в демилитаризованной зоне (DMZ); блокирование firewall входящих соединений со всеми портами, например, кроме http и https; предварительное планирование расширения сети и обозначения сегментов сети, способных к расширению; использование лицензионного ПО, желательно одного производителя; периодическое сканирование серверов для проверки отсутствия на нем уязвимых мест и др. И наиболее простой способ − это внимательное чтение лицензионных соглашений к программам, которые устанавливаются на компьютерах, подключенных к серверу.

Безопасность на должном уровне всегда требует больших затрат, тем не менее, с точки зрения эффективности, эти затраты себя в полной мере окупают. Приблизительные оценки расчета затрат для крупных компаний указывают на то, что возврат средств окупается в объеме 145% за три года. Но это субъективные и теоретические оценки. Многие компании, организующие безопасность, сегодня предлагают специальную услугу − проверку сервера на устойчивость к атакам хакеров, то есть определение наличия рисков. А при помощи он-лайн-формы можно оценить ROI от внедрения системы безопасности для вашего собственного предприятия. ROI (Return Of Investment) − это количественная оценка прибыли на инвестированный капитал. Необходимо четко знать следующие данные: количество обращений в службу сервиса в месяц; число рабочих мест, требующих установки ПО; стоимость таких действий, как вызов, оборудование защитой различных уровней; уменьшение числа обращений в службу сервиса на каждом из уровней и ряд других. В форме по умолчанию предложены определенные показатели, которые считаются образцовыми для предприятий.

Безопасность детерминирована такими категориями, как люди, процессы, программы. Это непрерывный поиск уязвимых мест системы, налаженная структура ликвидации угрозы и контроль над исполняемыми приложениями.

Литература: 1. Ефремов А. Иерархия защиты веб-серверов. – К.: Белый лист, 2007. – 112 с. 2. Федотов А. М. Проблемы безопасности информации в www-информационных системах. – К.: Академия, 2005. – 146 с. 3. Петров В. В. Как выбрать www-сервер. – К.: МК-Пресс, 2004. – 96 с. 4. Казеннов М. С. Безопасность www-серверов.– К.: КНД, 2006. – 344 с. 5. Фленов М. Web-сервер глазами хакера. − К.: МК-Пресс, 2006. – 156 с. 6. Бормотов С. В. Системное администрирование на 100 % / С. В. Бормотов, С. В. Бондаренко. – К., М.: 2007. – 162 с. 7. Медведовский И. Д. Атака через INTERNET/ И. Д. Медведовский, П. В. Семьянов, В. В. Платонов – К.: Метропресс, 2006. – 12 с.

Белецкий А. Я.

Белецкий А. А.

УДК 519.711/.72

СИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ШИФРОВАНИЯ

В классе симметричных криптоалгоритмов различают блочные и поточные шифры. В первой части работы рассмотрена достаточно гибкая к изменению параметров шифрования (размеров блоков и ключей) симметричная блочная криптосистема, названная системой RSB-32 [1; 2]. Основными для криптоалгоритма являются раундовые преобразования (Raund), разбитые на определенное число шагов (Step), а действие алгоритма осуществляется над блоками (Block) открытого или закрытого текстов, причем размер раундового ключа (как элемента общего ключа) составляет 32 бита. ***RSB*** − это итерационный блочный шифр, который доставляет уникальную возможность по изменению как размеров секретных ключей, так и числа шагов (раундов) шифрования.

В качестве криптографических примитивов в RSB алгоритме используются стохастические операции круговой прокрутки, скользящего кодирования, нелинейной замены и перестановки байтов, причем перечисленные криптопреобразования управляются в каждом блоке индивидуальными блочными раундовыми ключами, зависящими не только от значения секретного базового раундового ключа, но и всего текста, предшествующего преобразуемому блоку.

При шифровании больших объемов данных в реальном времени (таких, например, как речь или □живое видео□) применяются поточные криптографические системы (шифры, генераторы). Суть поточных шифров заключается в сложении по mod 2 битов потока ключей с битами сообщений. В современных криптосистемах поток ключей (поточный ключ) генерируется из короткого основного (базового) ключа с помощью однозначно определенных детерминированных алгоритмов, осуществляющих процедуру разворачивания ключа. В работе предлагается так называемое SPB семейство поточных криптографических алгоритмов систем, размер секретного ключа которых составляет 128 бит. Отличительная особенность SPB генераторов состоит в том, что за один шаг шифрования в системе формируется блок гаммы размером 128 или 64 бит, образующийся в результате стохастических операций нелинейной подстановки (Substitution) и перестановки

(Permutation), дополненные операциями стохастического сдвига и так называемого SX-преобразования.

Приводятся такие сравнительный анализ эффективности (по критерию качества статистических свойств псевдослучайных последовательностей) предлагаемых криптографических алгоритмов.

Литература: 1. Белецкий А. Я. Анализ эффективности симметричных криптоалгоритмов / А. Я. Белецкий, А. А. Белецкий // Електроніка та системи управління. – 2005. – №2(4). – С. 17 – 24. 2. Белецкий А. Я. Симметричный блочный RSB-32 криптоалгоритм / А. Я. Белецкий, А. А. Белецкий // Захист інформації. – 2006. – №2. – С. 42 – 50.

УДК 004.056

Семченко Д. А.

Замула А. А.

МЕТОДЫ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ НА ОСНОВЕ ПРОВЕДЕНИЯ ТЕСТОВ

Сложность сетевой инфраструктуры, многообразие данных и приложений приводят к тому, что при реализации системы информационной безопасности (ИБ) за пределами внимания администратора безопасности могут остаться многие угрозы. Основой для нападения злоумышленника являются системы сетевой защиты, серверы сети, доступ RAS-точки (например, модемы) и беспроводные сети. Для достижения необходимого уровня ИБ необходимо проведение регулярного тестирования систем на предмет устойчивости к атакам со стороны злоумышленника, социального инжиниринга и атак, направленных на обход технических мер и методов защиты [1].

В работе приведены основные шаги, осуществляющиеся при проведении теста на проникновение в корпоративную сеть, такие, как подготовка к тестированию (постановка целей тестирования, определение возможностей системы и т. д.), сбор информации о цели (краткий обзор установленных систем, структура сети и т. д.), анализ информации и рисков (анализ собранной информации, полученной на предыдущих этапах), активные попытки вторжения, конечный (заключительный) анализ [2].

Данный подход предполагает использование модулей двух типов:

I-модули (модули разведки) и E-модули (модули попыток проникновения) [2]. Модули, которые не могут быть выполнены в выбранном администратором безопасности подходе, должны быть исключены из теста.

Для получения полных результатов тестирования необходима комбинация различных тестов, которые описаны шестью критериями: информационная основа (начальный уровень знания о системе злоумышленником), агрессивность, возможности (проверка каких систем необходима), подход (скрытность проведения тестирования), методика и начальный этап (внешнее вторжение или атака изнутри сети).

В работе сформулированы цели, которые могут быть достигнуты проведением тестирования, такие, как: улучшение защиты технических систем; идентификация уязвимостей; наличие IT-защиты, подтвержденной внешним третьим лицом и улучшение организационной защиты [3].

Даётся также характеристика параметров, которые оказывают влияние на процесс тестирования корпоративной сети, в частности, время проведения тестирования (проведение лишь одного такого теста может занять более 20 дней), стоимость процесса тестирования, эффективность тестирования (полнота и адекватность системы защиты угрозам информационной безопасности, атакам со стороны злоумышленника).

Авторами приведены практические рекомендации по использованию методов тестирования и обеспечению безопасности корпоративной сети организации.

Литература: 1. Горбенко І. Д. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник / І. Д. Горбенко, Т. О. Гріненко. – Харків: ХНУРЕ, 2004. – 368 с. 2. BSI Federal Office for Information Security “A Penetration Testing Model”: Study 3. Галицкий А. В. Защита информации в сети / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М.:ДМК Пресс, 2004 – 616 с.

Борисенко А. А.

Кулик И. А.

УДК 681.32

БИНОМИАЛЬНАЯ ЗАЩИТА ИНФОРМАЦИИ

Широкое распространение сетей передачи данных и интенсивное внедрение информационных технологий в такие области, как промышленность, торговля, банковская деятельность и т. д., привело к необходимости защиты передаваемой и хранимой информации от несанкционированного доступа.

В настоящее время существует большой выбор различных методов защиты информации, каждый из которых обладает своими достоинствами и недостатками. Среди них достаточно известны методы, основанные на нумерационном кодировании, достоинством которого является то, что они наряду с защитой информации осуществляют также и её сжатие [1; 2]. Это, в свою очередь, дополнительно повышает стойкость шифрования данных.

Одним из таких методов нумерационного кодирования является метод нумерации на основе биномиальных чисел [3; 4]. Числовая функция двоичной биномиальной системы счисления, в рамках которой рассматриваются биномиальные числа N_j, $j = 0,1,...,C_n^k - 1$, имеет следующий вид:

$$N_j = x_1 C_{n-1}^{k-q_1} + x_2 C_{n-2}^{k-q_2} + ... + x_i C_{n-i}^{k-q_i} + ... + x_r C_{n-r}^{k-q_r} = \sum_{i=1}^{r} x_i C_{n-i}^{k-q_i},$$

где n и k – параметры двоичной биномиальной системы счисления;

x_i – биномиальная двоичная цифра – 0 или 1;

i – порядковый номер разряда, $i = 1,2,\ldots,r < n$;

r – длина двоичного биномиального числа;

q_i – сумма единичных цифр x_i от 1-го разряда до $(i-1)$-го включительно:

$$q_i = \sum_{t=1}^{i-1} x_t,\ q_i \le k\ .$$

Достоинством рассматриваемого метода нумерации, прежде всего, является простота шифрования, которая сводится к защите ключей, а не всего сообщения. Без этих ключей сообщения не могут быть расшифрованы. Сами ключи обладают длиной во много раз меньшей, чем в целом всё сообщение, и поэтому защитить их намного легче.

Другим достоинством предлагаемого метода защиты является то, что при реализации нет необходимости специально преобразовывать двоичное сообщение в биномиальное число. Достаточно подсчитать число единиц, содержащихся в двоичном сообщении, чтобы затем получить и биномиальное число, и ключ. Это значительно упрощает процедуры шифрования и дешифрования данных.

Таким образом, предлагаемый метод биномиальной защиты информации обладает простотой кодирования и декодирования и в то же время приводит к высокой стойкости шифра, использующего биномиальные числа. Кроме того, наряду с задачей защиты информации данный метод позволяет уменьшить объем передаваемых данных, что, в свою очередь, дополнительно увеличивает стойкость к раскрытию их содержания и уменьшает время на их перехват.

Литература: 1. Амелькин В. А. Методы нумерационного кодирования. – Новосибирск: Наука, 1986. – 156 с. 2. Хаффман Л. Дж. Современные методы защиты информации. – М.: Советское радио, 1980. – 262 с. 3. Борисенко А. А. Защита информации на основе сжатия // Вестник Сумского государственного университета. – 2006. – №4(88) – С. 53 – 55. 4. Борисенко А. А. Биномиальный счет. Теория и практика биномиального счета: Монография. – Сумы: ИТД "Университетская книга", 2004. – 170 с.

Секція 3
Інформаційні та телекомунікаційні системи в бізнесі

УДК 621.396.6. 519.2

Кравчук О. І.

ТРАНСФОРМАЦІЯ ПРИЗНАЧЕННЯ СКЛАДОВИХ ІНФОРМАЦІЙНО-ДОВІДКОВИХ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Розгортання досліджень для супроводження заходів Програми модернізації та розвитку озброєння й військової техніки (ОВТ) потребують значної концентрації зусиль у межах визначених цільових програм. Але, незважаючи на значні зусилля, що прикладаються, результатів досі не отримано. Спроби впровадження в Збройних силах України технічного обслуговування ОВТ за станом із застосуванням класичних підходів призвели до погіршення стану ОВТ та низки техногенних катастроф. Одним із підходів до організації експлуатації складних технічних систем, який запропоновано наприкінці 80-х років є формування теорії забезпечення експлуатації як альтернативи класичної теорії надійності. Для управління технологічними процесами зберігання, обслуговування та відновлення стану складних технічних засобів упроваджуються інформаційно-довідкові автоматизовані системи (ІДАС) підтримки прийняття рішень. Розвиток складових ІДАС є вельми актуальним завданням.

Визначення ІДАС подано в джерелі [1], це – система автоматизованої реєстрації, переробки, збереження й видачі інформації, що призначена для забезпечення абонентів відомостями довідкового характеру. Класична структура ІДАС передбачає три основні компоненти: технічне оснащення, математичне забезпечення і інформаційну базу. На основі визначення розроблено структурну схему ІДАС [2].

Технічне оснащення передбачало електронні обчислювальні машини (ЕОМ) та суміжні з нею засоби зберігання, передачі та відображення інформації. Передбачалось, що інформаційна база – це сукупність довідкових масивів, в яких зберігається інформація, а також комплекс алгоритмів, програм, набір формалізованих мов, операційна система і т. п.

На цей час в умовах суцільної комп'ютеризації усіх галузей діяльності завдання розроблення сукупності математичних процедур, розрахункових співвідношень, які у поєднанні із сучасним ПЕОМ є засобом для створення автоматизованих робочих місць осіб, що приймають рішення [2], трансформуються в завдання безпосереднього створення ІДАС. Сучасні ІДАС створюються у вигляді програмного продукту під конкретний вид ПЕОМ з операційною системою, тобто математичне забезпечення та інтерфейс реалізовані у програмному продукті.

Робоче місце організовується шляхом створення програмного продукту для реалізації інформаційних моделей, що описують реальні фізичні процеси. Інформація про динаміку зміни цих процесів складає зміст інформації, необхідної для прийняття рішення. Програмний продукт з класичного змісту, що подано в джерелі [1], трансформувався у сукупність процедур обробки інформації та інтерфейсів для розуміння, формалізації завдань і прийняття рішення для управління технологічним процесом, що автоматизується [3].

Враховуючи сучасний розвиток комп'ютерних технологій, забезпеченість організацій, установ комп'ютерною технікою і за умовами наявності інформаційної бази, можемо зробити висновок, що сучасна ІДАС становить сукупність математичних процедур, реалізованих у вигляді програмного продукту з відповідним інтерфейсом для розгалужених операційних систем ПЕОМ (Windows, Unix, Linux і т.і.).

Література: 1. Словарь по кибернетике / Под ред. В. С. Михалевича. – 2-е изд. – К.: Гл. ред. УСЭ им. М. П. Бажана, 1989. – 752 с. 2. Кравчук О. І. Функціонування інформаційно-довідкової системи визначення стану радіоелектронних засобів під час багаторежимного утримання // Тематичний збірник „Системи обробки інформації" – 2008. – Вип. 3 – С. 48 – 51. 3. Кравчук О. І. Завдання синтезу інформаційно-довідкової автоматизованої системи як елементу експертних систем прийняття рішення про технічний стан ОВТ // Зб. наук. пр. Одеського інституту Сухопутних військ. – 2007. – № 14. – Ч. 2. – С. 57 – 60.

Баранник В. В.

Карпенко С. В.

УДК 621.327:681.5

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ТРЕХУРОВНЕВОГО ДЕКОДИРОВАНИЯ

Характерной особенностью информационных систем является обработка и передача изображений. При этом для повышения степени достоверности получаемой информации их размеры постоянно увеличиваются [1]. Значит, сокращение времени доведения информации основывается на: повышении степени сжатия изображений и уменьшении времени их обработки. В случае трехмерного полиадического кодирования достигается дополнительное увеличение степени сжатия относительно двумерной обработки [2–3]. Однако время обработки увеличивается. Следовательно, для снижения суммарного времени трехмерной обработки необходимо сократить время кодирования и декодирования. Отсюда цель исследований заключается в разработке параллельного трехмерного декодирования видеоданных, обеспечивающего уменьшение времени восстановления без внесения погрешности.

Разработка трехуровневого параллельного трехмерного декодирования. Схему восстановления [3] трехмерной структуры данных (ТСД) можно разбить на последовательность типовых операций восстановления укрупненных элементов: по строкам и вертикалям, по вертикалям и непосредственное восстановление элементов ТСД. Для уменьшения количества операций предлагается разработать трехуровневую параллельную схему восстановления трехмерных чисел. Трехмерная параллельная схема реализации трехмерного полиадического декодирования заключается в том, что восстановление элементов различных уровней ТСД осуществляется сразу, как только получен соответствующий код-номер. Структура данных разделяется логически на три следующих уровня: первый уровень состоит из кодов-номеров, сформированных для укрупненных элементов ТСД по строкам и по сечениям; второй уровень образуется из кодов-номеров, построенных для отдельных вертикалей ТСД; третий уровень формируется непосредственно из элементов трехмерной структуры данных.

Отличительной особенностью трехуровневого параллельного восстановления от одноуровневого восстановления состоит в возможности проводить восстановление ТСД по мере вычисления накопленного произведения оснований обработанных элементов трехмерных чисел. С учетом указанной особенности для реализации параллельного трехуровневого восстановления на каждом уровне обработки требуется выполнить три операции деления одну операцию умножения и одну операцию вычитания. Поскольку всего три уровня обработки, то на восстановление всей ТСД потребуется затратить 9 операций деления, 3 операции умножения и 3 операции вычитания. Экспериментальные оценки показывают, что трехуровневое параллельное восстановление позволяет относительно одноуровневого параллельного восстановления элементов трехмерных чисел снизить дополнительно время обработки в среднем в 2 раза.

Таким образом:

1. Создана трехуровневая параллельная реализация трехмерного полиадического декодирования. Трехмерная параллельная схема реализации трехмерного полиадического декодирования заключается в том, что восстановление элементов различных уровней ТСД осуществляется сразу, как только получен соответствующий код-номер.

2. Трехуровневое параллельное восстановление позволяет относительно одноуровневого параллельного восстановления элементов ТПЧ снизить дополнительно время обработки в среднем в 2 раза.

Литература: 1. Ватолин В. И. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / В. И. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ – МИФИ, 2002. – 384 с. 2. Баранник В. В. Сжатие данных на основе сокращения трехмерной структурной избыточности / В. В. Баранник, С. В. Карпенко // Открытые информационные и компьютерные интегрированные технологии. – 2007. – Вып. 37. – С. 27 – 34. 3. Карпенко С. В. Создание подхода для исключения трехмерной избыточности изображений // Зб. наук. пр. – Харків: ХУ ПС. – 2007. – Вип. 3(15). – С. 2 – 5.

УДК 004.652

Берко А. Ю.

ІНТЕГРАЦІЯ РІЗНОРІДНИХ ДАНИХ У СИСТЕМАХ ЕЛЕКТРОННОГО БІЗНЕСУ

Створення та запровадження систем електронного бізнесу сьогодні є одним із перспективних і динамічних напрямів розвитку галузі інформаційних технологій. Найважливішими перевагами систем електронного бізнесу є відсутність громіздкої та дорогої інфраструктури, а також реалізація значної частини бізнес-функцій засобами телекомунікаційних та інформаційних технологій. Серед великої кількості систем електронного провадження бізнесу особливе місце займають системи створення та поширення продуктів інформаційних технологій, в яких основним ресурсом є дані, а результатом – інформаційні продукти та інформаційні сервіси. Однією з важливих проблем розроблення та застосування таких систем є організація інформаційних ресурсів. У загальному випадку він складається як із структурованих реляційних даних, збережених у БД, так і з великої кількості даних, поданих у довільному форматі – слабкоструктурованих даних. Для ефективного функціонування системи електронного бізнесу важливо забезпечити інтеграцію різнорідних компонентів інформаційного ресурсу та забезпечити їх сумісне застосування.

За оцінками експертів лише близько 20 відсотків інформаційного ресурсу в сучасних системах електронного бізнесу зберігається в базах даних у вигляді структурованої інформації, решту складають дані, подані у різноманітних форматах без попередньо визначеної чіткої структури – так звані слабоструктуровані дані [1].

У загальному випадку, до категорії слабкоструктурованих даних відносять: напівструктуровані дані, структура яких є непостійною, або неоднозначною, самоструктуровані дані, структуру яких визначають за допомогою їх самих та дані, структуру яких попередньо не встановлено, і її визначають в процесі інтерпретації даних. Зберігають такі дані у формі текстових файлів, файлів документів, XML-документів, Web-сторінок, графічних і мультимедійних файлів тощо. Різноманітність форм і структури інформаційного ресурсу, у свою чергу, викликає необхідність розроблення методів і технологій, які забезпечують спільне, узгоджене опрацювання і застосування таких неоднорідних даних.

Якщо в складі інформаційного ресурсу системи електронного бізнесу присутні структуровані (реляційні) та слабкоструктуровані елементи, то його узагальнену модель можна подати як деякий кортеж виду:

$$C=<R, S1, S2, \ldots, Sk, JR, JS, JRS>,$$

де C – схема інтегрованого інформаційного ресурсу;
R – схема реляційної складової, яку утворюють структуровані дані, подані у вигляді таблиць БД;
$S_1, S_2, \ldots, S_k$ – схеми слабкоструктурованих складових різного типу,
JR – множина зв'язків між реляційними елементами;
JS – множина зв'язків між слабкоструктурованими елементами;
JRS – множина зв'язків між реляційними та слабкоструктурованими елементами.

Запропонована модель дає можливість побудувати узагальнений опис всіх видів і категорій даних, які утворюють інформаційний ресурс систем електронного бізнесу, що, у свою чергу, дозволяє розробляти методи та засоби організації та опрацювання неоднорідних наборів даних. Основні проблеми інтеграції баз даних з іншими типами даних, а також напрями й принципи їх вирішення визначено, зокрема, в джерелах [2–3].

Розроблення методів та засобів для розв'язання комплексу задач інтеграції різнорідних інформаційних ресурсів сьогодні вважають одним із важливих та перспективних напрямів розвитку сучасних інформаційних технологій. Значною мірою проблеми, повязані з побудовою інтегрованих середовищ опрацювання реляційних та слабкоструктурованих даних сьогодні реалізовано у сучасних версіях систем управління базами даних провідних виробників, а також у спеціалізованих системах управління контентом.

Література: 1. Литовский К. Ю. Слабоструктурированные данные: некоторые методы их представления и обработки запросов/ К. Ю. Литовский, Г. С. Томусяк // Московская Секция ACM SIGMOD. – 2000. – С. 1 – 2. – // http:// synthesis.ipi.ac.ru/ sigmod/seminar/s20000224. 2. The Lowell Database Research Self-Assessment Meeting [Електронний ресурс]/ Lowell Massachusetts. – 4-6 May 2003 // http://research.microsoft. com/ ~gray/ lowell. – June, 2003. 3. Берко А. Ю. Методи інтеграції даних в інформаційних системах на основі XML-технологій/ Андрій Берко// Міжвідомчий збірник наукових праць. "Відбір і обробка інформації".– 2007. – №. 27(103). – С. 116 – 121.

Марьяновський В. А.

Юштін К. Е.

УДК 519.7

АВТОМАТИЗАЦІЯ СИНХРОННОГО УПРАВЛІННЯ НАВЧАЛЬНО-МЕТОДИЧНИМ ПРОЦЕСОМ У ВНЗ

Складність управління навчальним процесом полягає в тому, що оцінка якості управління та коригування навчальних планів, перерозподіл навантаження, покращення розкладу занять можливі тільки після завершення певного циклу навчання (семестру, навчального року і т. п.). Таке управління називається асинхронним на відміну від управління об'єктом у довільний момент часу, яке визначається як синхронне управління. При синхроному управлінні здійснюється корекція поведінки об'єкта під впливом органів управління, а при асинхроному управлінні – вибір набору та послідовності операцій, виконання яких має привести до деякої цілі, оцінка якої отримується після завершення чергового етапу процесу.

Навчальний процес як система взаємодії об'єктів у часі описується трьома групами об'єктів: викладачі, навчальні групи й аудиторії, які використовуються для досягнення визначеної цілі у вигляді деякого технологічного процесу, що описується заданим навчальним планом. Оскільки множини значень зазначених груп досить потужні, пошук оптимального за деякою сукупністю критеріїв варіанта управління їх взаємодією є трудомістким процесом і потребує автоматизації.

Навчальний процес, з точки зору управління об'єктами в умовах обмежених ресурсів, може бути розділений на три основних етапи.

Перший етап – етап планування, на якому можливе виділення двох складових частин – планування навчального навантаження, тобто закріплення навчальних занять в групах за конкретними викладачами, і планування поведінки процесу, тобто розподіл занять у часі (складання розкладу).

На другому етапі безпосередньо здійснюється навчальний процес. У період виконання цього етапу можливі відхилення від початкових значень складу викладачів, аудиторного фонду, груп студентів. Керування на цьому етапі зводиться до мінімізації втрат від цих відхилень без зміни загального розкладу. Мінімізація цих втрат може бути спланована на етапі складання розкладу при обліку критеріїв стійкості розкладу до таких відхилень.

На третьому етапі виробляється оцінка результатів планування і виконання навчального процесу. Ця оцінка має дві складові: оцінка рівня досягнення мети навчання й оцінка якості розкладу. У першому випадку оцінюється навчальний план (інакше набір операцій) і приймається рішення про якість навчання. В другому – оцінюється сам розклад з погляду ергономічних показників, стійкості і тому подібне і можуть бути вироблені критерії для побудови розкладу на наступний період роботи.

Відповідно до запропонованої схеми керування навчальним процесом можна виділити дві області, в яких автоматизація управління є важливою і суттєво необхідною: це етап складання розкладу і розрахунок часткової та узагальненої оцінок результату навчального процесу.

Процес складання розкладу навчальних занять характеризується значною трудомісткістю і, у даний час, часто спрямований на задоволення умови несуперечності навчальних занять, тобто на перевірку того, що викладачі, групи студентів і аудиторії зайняті в обраний час тільки одним заняттям навчального процесу. Для розв'язку задачі формування та покращення розкладу, яка розглядається як багатокритеріальна та багатофакторна задача оптимізації, може бути запропонований ряд процедур і методів вибору оптимальних рішень на основі послідовного аналізу варіантів, методу гілок і меж, пошукові процедури і т. ін. Але при реалізації зазначених процедур на ЕОМ, як правило, не вирішеною залишається головна проблема задачі – це значна тривалість автоматизованого процесу складання розкладу.

Друга область автоматизації – це розрахунок часткової та узагальненої оцінок результату навчального процесу. Вибір локальних критеріїв і вигляду загального критерію залежить від фахівця (людини, що приймає рішення, – ЛПР). Цей підхід є добре формалізованим у теорії багатокритеріального вибору та прийняття рішень. Як загальний критерій можуть бути обрані різні адитивні або мультиплікативні форми, використано нечіткий підхід. Однак остаточне рішення про вигляд загального й часткових критеріїв залежить від конкретного ЛПР.

Деякі розглянуті вище проблеми розробки автоматизованих підходів в організації навчального процесу розглянуто та формалізовано в процесі створення та впровадження в Київському національному університеті імені Тараса Шевченка системи управління базою даних "Студент".

Література: 1. Івохін Є. В. Використання електронних засобів в організації навчального процесу в Київському національному університеті імені Тараса Шевченка / Є. В. Івохін, К. Е. Юштін, Д. О. Вадньов / Зб. ст. "Актуальні проблеми міжнародних відносин", Ч.ІІ. – К.: ІМВ., 2002. – С. 240 – 247. 2. Косинський К. О. Інформаційно-аналітична система забезпечення управління роботою наукових підрозділів у ВНЗ / К. О. Косинський, К. Е. Юштін // Управління розвитком. – №3. – 2007. – С.158.

УДК 621.327:681.5

Баранник В. В.

Яковенко А. В.

МЕТОД ИСКЛЮЧЕНИЯ ИЗБЫТОЧНОСТИ В ТРАНСФОРМАНТАХ УОЛША

Развитие информационных систем связано с расширением спектра видеоинформационного обеспечения [1]. Актуальной научно-прикладной проблемой, требующей своего решения, является увеличение степени сжатия изображений с заданным уровнем достоверности информации [2; 3]. Существующие технологии компрессии видеоданных, обеспечивающие наибольшие степени сжатия, строятся на базе методов, осуществляющих устранение психовизуальной избыточности [2; 3]. Проявляется противоречие между коэффициентом сжатия и степенью потерь информации. Поэтому цель исследований заключается в построении технологии компрессии видеоданных с контролируемой погрешностью.

Особенности технологии компрессии. Построение технологии компрессии изображений базируется на следующих методологических принципах:

1) разработка метода компактного представления видеоданных, включающего в себя комплекс подходов для устранения избыточности изображений и формирование кодограмм их сжатого представления;

2) создание методики формирования параметров процесса сжатия изображений, обеспечивающей достижение максимального эффекта от реализации разработанного метода.

Первый методологический принцип характеризуется тем, что:

сжатие видеоданных обеспечивается за счет устранения комбинаторной и психовизуальной избыточности в трансформантах двумерного преобразования Уолша;

используется математический аппарат двумерных ортогональных преобразований и методов структурного кодирования;

формирование кодограмм проводится для вычисленного значения кода-номера двумерного плавающего полиадического числа. Значение кода-номера зависит от длины кодограммы, что позволяет реализовать принцип равномерности кодовых конструкций;

служебные данные несут информацию о структуре и формах изображений. Упаковка служебных данных проводится на основе кодирования без внесения погрешности.

В соответствии с первым принципом второй методологический принцип содержит формирование таких параметров, как:

размерность массивов видеоданных, на которые разбивается исходное изображение. При этом необходимо учитывать, что, с одной стороны, наибольшее значение степени концентрации энергии в трансформантах ДПУ достигается для двумерных локальных блоков с однородной структурной. С другой стороны, с ростом размеров блоков существует возможность для исключения потенциально большего количества избыточности;

фактор качества, влияющий, с одной стороны, на количество сокращаемой психовизуальной избыточности, а, с другой стороны, на качество восстанавливаемых изображений. Для этого необходимо проанализировать возможность дополнительной квантизации компонент трансформант и возможные варианты нормировки их значений;

длина кодограммы. Данный параметр влияет на: степень сжатия, так как управляет количеством компонент трансформант, для которых вычисляется один код; время обработки, поскольку появляется возможность изменять количество обращений к внешней памяти и количество машинных операций;

структурные характеристики процессов устранения избыточности при упаковке служебных данных.

Таким образом, построенный метод позволяет дополнительно сократить избыточность трансформант в среднем на 50%.

Литература: 1. Уолрэнд Дж. Телекоммуникационные и компьютерные сети. – М.: Постмаркет, 2001. – 480 с. 2. Exploiting Hyperspectral Imagery // IEEE Signal Processing Magazine. – 2002. – Vol. 19. – №1. – 80 p. 3. Ватолин В. И. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / В. И. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ – МИФИ, 2002. – 384 с.

Знахур С. В.

Мисюра О. Н.

УДК 681.620:518

ОСНОВЫ ПОСТРОЕНИЯ РАСПРЕДЕЛЕННОЙ ПОИСКОВОЙ СИСТЕМЫ

Эффективность экономики, основанной на знаниях, всецело зависит от эффективности производства и использования знаний. Для экономики знаний важны и необходимы как процесс порождения знаний, так и процесс их распространения. Стремительное развитие глобальных информационных и вычислительных сетей ведет к поддержке и развитию распределенных информационно-вычислительных ресурсов.

При формировании единого информационного пространства были приняты следующие основные принципы [1]:

иерархичность информационных систем и ресурсов;

разнородность ресурсов и программно-технологических сред, объединяемых в едином пространстве.

На настоящий момент в основу единого информационного пространства положен принцип самоорганизации, где участники организуются в группы на добровольной основе. Схема реализации механизмов поиска в едином информационном пространстве может быть реализована на основе использования метаданных и по содержанию информационных ресурсов. Поиск по единому информационному пространству основан на том, что через единую точку доступа необходимо реализовать параллельный поиск по всем информационным ресурсам. Информационные ресурсы каждого участника единого информационного пространства должен быть снабжен стандартными метаданными и стандартным индексом представления содержания информационных ресурсов. Эти стандартные компоненты являются образами информационных ресурсов для выполнения поиска.

Следует отметить, что использование коммуникационной среды Internet и WEB-технологий позволяют обеспечить процессы распределения и глобализации информационных ресурсов. Однако имеющиеся информационно поисковые системы (ИПС) общего назначения не позволяют осуществить эффективный поиск требуемой информации в распределенных системах, поскольку большинство из них не в состоянии проиндексировать все WEB-пространство. Для обеспечения эффективной автоматической обработки информационных ресурсов предлагается использовать не сами ресурсы, а некоторые их описания – метаданные. В основу манипулирования метаданными, определяющими функциональные связи между документами, предлагается использовать схему RDF (Resource Description Framework, RDF-Schema).

При создании единой системы доступа к ресурсам должны быть решены следующие принципиальные задачи:

обеспечение релевантности информации;

диспетчеризация, включая идентификацию доступных ресурсов, статистика использования и загрузки ресурсов и пр.;

система безопасности и контроля доступа, гибкое регулирование объема прав и привилегий пользователей;

обращение к наборам данных в удаленных архивах (включая протоколы, которые необходимо использовать для работы с гетерогенными источниками данных, и библиотеки программных комплексов).

Таким образом, организация данных в ИПС для распределенных сетей и GRID-сетей основана на взаимодействии следующих подсистем:

публикации данных, поддержка их аутентичности и качества;

поиска и представления информации;

анализа распределенных данных.

Эти подсистемы составят основу системы превращения информации в систему библиотек, оперирующих с документами. Следует отметить, что реализация подобной распределенной информационной системы позволит перейти к построению интеллектуальной системы обработки запросов, основанной на распознавании образов документов.

Механизм работы ИПС следующий. Полученный от приложения запрос направляется в систему обработки, которая посредством системы поиска информации разыскивает необходимые данные и после выполнения удаленных процедур. Система обмена метаданными основывается на сервере метаданных, который поддерживает следующий набор служб:

публикация/регистрация новых наборов данных;

база метаданных для поиска данных по атрибутам;

доступ к гетерогенным ресурсам посредством брокера ресурсов;

контроль аутентификации и доступа;

мониторинг информационных ресурсов и ресурсов ввода/вывода;
распределенное исполнение служб.

Таким образом, реализация ИПС для распределенных систем базируется на метамодели, которая описывает документ, как набор присущих ему атрибутов и методов, характеризующих связи с другими документами. Информация о документах системы, их атрибутах и методах поддерживается сервером метаданных. Сервер метаданных является отдельной частью системы, содержащей описание информационной модели предметной области, параметров настройки стандартных функций системы. Реализация метамодели возможна на основе использования стандартов платформы XML. Для этих целей могут использоваться как средства самого языка XML (описание типов документов DTD), так и языковые средства стандартов XML Schema и RDF.

Таким образом, средства поиска для распределенных систем должны поддерживать интерфейсы с широким диапазоном гетерогенных источников, быть совместимыми с соответствующими протоколами поиска и извлечения ресурсов, быть способными обрабатывать широкий диапазон типов ресурсов и форматов (например, XML, RDF), обеспечивать однородное представление результатов поиска, сортировку и ранжирование, исключение дубликатов. Средства запроса ресурсов должны использовать ясные методы запроса ресурсов из различных источников, используя требуемые протоколы, поддерживать управление правами доступа. Средства доставки ресурсов должны поддерживать совокупность методов доставки ресурсов, например, доставку текстов, мультимедийных данных по протоколам HTTP, SMTP.

Литература: 1. Шокин Ю. И. Информационная система Сибирского Отделения РАН / Ю. И. Шокин, А. М. Федотов // "Электронные библиотеки: перспективные методы и технологии, электронные коллекции". Сб. докл., Второй Всеросс. научн. конф., Протвино, 26–28 сентября 2000 г. – Протвино: ГНЦ, 2000.

УДК 004.056

Кислов А. А.

Короткина Л. А.

ПОСТРОЕНИЕ БЕЗОПАСНЫХ И ПРОИЗВОДИТЕЛЬНЫХ КОРПОРАТИВНЫХ СЕТЕЙ

Во избежание утечки информации (промышленный шпионаж), кражи электронных подписей и конфиденциальной информации, нарушения функционирования производственного процесса следует обеспечить безопасное функционирование корпоративной сети.

В ядре крупной корпоративной сети авторы предлагают использовать флагманское решение в области маршрутизации трафика, обладающее производительностью, достаточной для маршрутизации трафика полного канала E3 с физическим быстродействием линии. Порты Fast Ethernet и встраиваемый конвертер медь/оптоволокно позволят подключиться к основному поставщику услуг по городской сети Fast Ethernet, либо создавать в центральном офисе две изолированные физические сети (например, внутреннюю локальную сеть и отдельную сеть для размещения общедоступных Web-ресурсов).

При построении крупной безопасной корпоративной сети авторы считают уместным использовать следующие решения:

виртуальные частные сети (VPN) [1];
виртуальные локальные сети (VLAN) 802.1q;
механизмы обеспечения качества услуг (QoS) ToS/DiffServ, traffic shaping, traffic policing;
многоканальные IP-соединения;
режим моста Ethernet-over-Frame Relay, реализованного в виде Cisco-совместимых bridge groups;
сбор статистики в формате NetFlow;
расширенный набор протоколов динамической маршрутизации: RIP, RIP2, OSPF, BGP;
безопасный удаленный доступ на основе SSH/SSL;
программно и аппаратно реализованные брандмауэры.

Кроме того, авторы считают целесообразным использовать модемные модули SHDSL-bis, SHDSL, SDSL, IDSL [2], а также традиционные внешние модемы с последовательными интерфейсами (V.35 и др.). Предлагаем использовать современные технологии широкополосного местного доступа, например, модемы xDSL различных производителей, мосты радио-Ethernet, кабельные модемы и другое оборудование, оснащенное интерфейсами Ethernet. В качестве транспортной

среды также допускаем использовать каналы E1. Встраиваемые модемы GSM/GPRS и CDMA обеспечивают резервное, а при отсутствии проводных альтернатив и основное соединение с Интернет или корпоративной сетью по сотовой сети.

К одному из портов (как правило, встроенному Fast Ethernet) подключается локальная сеть офиса, закрытая для доступа извне; к другому − канал от поставщика услуг Интернет; к третьему − так называемая "демилитаризованная зона", то есть изолированная физическая сеть, в которой размещаются общедоступные Web-ресурсы: серверы HTTP, FTP, электронной почты и т. п.

Классическая схема построения корпоративных сетей подразумевает объединение локальных сетей офисов (2-го уровня) на третьем уровне − уровне межсетевого взаимодействия, что и отражено в его названии: internetworking layer. Именно эта задача решается с помощью маршрутизаторов. Однако по мере распространения широкополосных каналов связи растет популярность альтернативного решения − прозрачного объединения локальных сетей при помощи мостов второго уровня. Выбор сводится к сопоставлению затрат на более "интеллектуальное" оборудование (разовые расходы) и более квалифицированного сетевого администратора (регулярные расходы), с одной стороны, и регулярных расходов на аренду или владение высокоскоростными каналами связи, в другом. С одной стороны, технологии второго уровня привлекают пользователей простотой конфигурации и возможностью прозрачной работы сетевых приложений в пределах всей "растянутой" сети без дополнительной настройки. С другой стороны, узкополосные каналы WAN могут быть с большой вероятностью перегружены широковещательным трафиком LAN до такой степени, что прохождение полезного трафика станет невозможным [3].

Причинами снижения производительности или полной неработоспособности приложений LAN в глобальных сетях являются: большое время обращения пакетов, увеличенный процент ошибок и потерянных пакетов и т. п. Использовать технологии LAN для объединения сетей возможно исключительно тогда, когда характеристики каналов WAN приближаются к характеристикам локальной сети [4].

Литература: 1. Кульгин М. В. Компьютерные сети. Практика построения. Для профессионалов. 2-е изд. – К.: Питер, 2003. – 390 с. 2. Бакланов И. Г. Технологии ADSL / ADSL2 +. Теория и практика применения. – К.: Метротек, 2007. – 204 с. 3. Конахович Г. Ф. Сети передачи пакетных данных / Г. Ф. Конахович, В. М. Чуприн. – К: МК-Пресс, 2006. – 260 с. 4. Дж. Ирвин. Передача данных в сетях: инженерный подход / Дж. Ирвин, Д. Харль. – К.: BHV, 2003. – 410 с. 5. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. – К.: Академия, 2006. – 194 с. 6. Гринфилд Д. Оптические сети. – К.: Диасофт, 2002. – 115 с. 7. Архипкин В. Я. Bluetooth. Технические требования. Практическая реализация. Приложения / В. Я. Архипкин, А. В Архипкин. – К.: Мобильные коммуникации, 2004. – 132 с. 8. Naoki Wakamiya, Marcin Solarski, James Sterbenz. Active Networks / Naoki Wakamiya, Marcin Solarski, James Sterbenz. – К.: IWAN, 2004. – 157 с.

Кравець П. О.

УДК 004.852; 004.942

ІГРОВА МОДЕЛЬ РИНКУ ЦІННИХ ПАПЕРІВ ТА ІНВЕСТИЦІЙ

Модель ринку цінних паперів та інвестицій є одним із різновидів економічних моделей збалансованого обміну ресурсами [1]. При цьому важливим є врахування факторів невизначеності та стохастичної природи економічної системи в умовах ринкової конкуренції, які здійснюють значний вплив на динаміку поведінки системи.

В умовах невизначеності учасникам ринку апріорі не відомі оптимальні стратегії купівлі-продажу акцій. Тому для зменшення ризику прийняття неефективних рішень, стратегії поведінки необхідно будувати на основі самонавчальних процедур, які враховують інформацію про передісторію кон'юнктури ринку цінних паперів. Враховуючи розподілений і конкурентний характер задачі, для її розв'язання пропонується стохастична ігрова модель [2].

Розглянемо L учасників ринку цінних паперів, кожен з яких володіє пакетом акцій $X^i \in R_+^m$, $i = \overline{1,L}$. Елемент $x^i(j) \in X^i$, $j = \overline{1,m}$ позначає кількість акцій j-го виду для і-го учасника.

Вступаючи у систему купівлі-продажу, і-й учасник може замінити свій пакет акцій з X^i на Y^i. Вважаємо, що обмін є збалансованим:

$$\sum_{i=1}^{L} X^i = \sum_{i=1}^{L} Y^i = Z = const\,. \qquad (1)$$

Нехай $C \in R_+^m$ – ціни на акції, які в загальному випадку можуть змінюватися залежно від кон'юнктури ринку. Тоді поточні витрати на придбання акцій дорівнюють:

$$\varphi^i = \left\langle C, Y^i - X^i \right\rangle,$$

де $\langle \bullet, \bullet \rangle$ – скалярний добуток векторів. Якщо $\varphi^i > 0$, то учасник торгів несе витрати на придбання акцій, а при $\varphi^i > 0$ – отримує прибуток від їх реалізації.

Для виконання операцій з акціями кожен учасник має капітал $K_i \geq 0$ і за необхідності може взяти у банку позику $\Delta_i > 0$ під відсоток $\alpha \geq 0$ для придбання акцій, або покласти вільну готівку $\Delta_i < 0$ у банк. Грошові операції банку з кредитним капіталом $K > 0$ повинні задовольняти умову:

$$\sum_{i=1}^{L} \Delta_i \leq K\,. \qquad (2)$$

Витрати φ^i не повинні перевищувати суми капіталу і-го учасника:

$$\varphi^i \leq K_i + \Delta_i\,,\ i = \overline{1,L}\,. \qquad (3)$$

Після завершення операцій розміщення капіталу кожен учасник отримує дивіденди $v^i(Y^i) \geq 0$, величина яких залежить від непередбачуваних факторів виробництва та збуту продукції.

Функціонування моделі здійснюється в дискретні моменти часу $n = 1,2,\ldots$. В кінці поточного кванту часу учасники підраховують прибуток

$$\xi_n^i = v_n^i(Y^i) - \varphi_n^i - (1+\alpha)\Delta_n^i\,,\ i = \overline{1,L}\,. \qquad (4)$$

Мета розв'язування задачі полягає у визначенні такої стратегії обміну $X_n^i \to Y_n^i$, яка забезпечує виконання системи цілей

$$\varliminf_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} \xi_t^i \to \max\,,\ i = \overline{1,L} \qquad (5)$$

при обмеженнях (1 – 3).

Нехай акт купівлі-продажу акцій здійснюється L гравцями. Кожен і-й гравець вибирає кількість акцій j-го виду з набору чистих стратегій $x^i(j) = (0,1,2,\ldots,N)$, $j = \overline{1,m}$, $N \geq 1$ за допомогою ймовірнісного механізму, побудованого на основі векторів змішаних стратегій $p^i(j) = (p_1^i(j), p_2^i(j), \ldots, p_N(j)) \in S^N$, які приймають значення на N-вимірному одиничному симплексі S^N [3].

Баланс (1) забезпечується проектуванням результатів вибору X^i на гіперплощину $\sum_{i=1}^{L} x^i(j) = Z$, $j = \overline{1,m}$, після чого отримуємо нові значення пакетів акцій Y^i, $i = \overline{1,L}$. Якщо $y^i(j) > x^i(j)$, то і-й гравець купує акції j-го виду. При цьому, якщо поточні витрати на придбання акцій перевищують значення його капіталу $\varphi^i > K_i$, то він бере кредит Δ_i у банку з дотриманням умови (3). Якщо загальна сума кредитів перевищує кредитний капітал банку $\sum_{i=1}^{L} \Delta_i > K$, то кожен гравець отримує тільки частину кредиту, обчислену в результаті проектування суми запитуваних кредитів на гіперплощину $\sum_{i=1}^{L} \Delta_i = K$.

Після обчислення поточних виграшів (4) здійснюється динамічний перерозподіл векторів змішаних стратегій за допомогою одного із рекурентних марківських методів [3]:

$$p_{n+1}^{i}(j)=\pi_{n+1}^{N}\left\{p_{n}^{i}(j)-\gamma_{n}R_{n}(x_{n}^{i}(j),p_{n}^{i}(j),\xi_{n}^{i}(j))\right\}\in S^{N},\ j=\overline{1,m},\ i=\overline{1,L}, \qquad (6)$$

де π_{n+1}^{N} – проектор на одиничний симплекс S^{N}; $\gamma_{n}\geq 0$ – крок методу;

$R_{n}(\bullet)\in R^{N}$ – вектор руху методу.

Для забезпечення системи цілей (5) вектори руху R_n будуються на основі стохастичної апроксимації [4] гіпотези індикаторної поведінки, градієнта або псевдоградієнта функції середніх виграшів.

Працездатність методів (6) забезпечується у класі монотонно спадних послідовностей величин γ_n та ε_n при обмеженнях, визначених теоремами теорії стохастичної оптимізації [5].

Умовою завершення стохастичної повторювальної гри є досягнення розв'язку задачі (5) з потрібною точністю.

Стохастичні ігри дають можливість будувати ефективні моделі ринкової економіки та розв'язувати задачі децентралізованого збалансованого розподілу ресурсів в умовах невизначеності. Розв'язки ігрової задачі визначаються базовими критеріями і відповідають умовам колективної оптимальності, наприклад, за Нешем, Парето та ін.

Література: 1. Пшеничный Б. Н. О существовании равновесных цен в общей модели производства и обмена / Б. Н. Пшеничный, Н. В. Полищук. Экономика и математические методы. – 1987. – Т. XXIII. – Вып 2. – С. 313 – 319. 2. Fudenberg, D. The Theory of Learning in Games / D. Fudenberg, D.K. Levine. – Cambridge, MA: MIT Press, 1998. – 292 p. 3. Назин А. В. Адаптивный выбор вариантов: Рекуррентные алгоритмы / А. В. Назин, А. С. Позняк. – М.: Наука, 1986. – 288 с. 4. Вазан М. Стохастическая аппроксимация. – М.: Мир, 1972. – 295 с. 5. Невельсон М. Б. Стохастическая оптимизация и рекуррентное оценивание / М. Б. Невельсон, Р. З. Хасьминский. – М.: Наука, 1972. – 304 с.

Коломійцев О. В.

Коваленко С. П.

УДК 681. 375

СЕЛЕКТОР ПОДОВЖНІХ МОД ІЗ БАГАТОЧАСТОТНИМ РОЗДІЛЕННЯМ КАНАЛІВ ДЛЯ ОБМІНУ ІНФОРМАЦІЄЮ З ЛІТАЛЬНИМ АПАРАТОМ

Сучасний високий рівень розвитку лазерної техніки і використання лазерного випромінювання відкриває широкі можливості для вирішення завдань як високоточного вимірювання параметрів руху (ВПР) літальних апаратів (ЛА), так і інформаційного обміну з ним. Такі можливості обумовлені, в першу чергу, використанням у лазерних інформаційно-вимірювальних системах (ЛІВС) джерел випромінювання на лазерах, що володіють великою частотою, яку несуть, і спектральною яскравістю, монохроматичністю, просторовою та часовою когерентністю. Завдяки цьому в ЛІВС можливе формування понадвузьких діаграм спрямованості (ДС) (~10^{-4} рад) і отримання великих коефіцієнтів посилення при порівняно малих оптичних антенах. Лазерні джерела випромінювання дозволяють генерувати потужні імпульси з ультракороткою тривалістю, що забезпечують якісний взаємозв'язок і високу точність ВПР ЛА [1]. При цьому, якщо врахувати той факт, що існуючі ЛІВС [2], використовують імпульсний характер сигналу, але не враховують його багаточастотність, то не може бути й мови про достатню багатоканальність обміну інформацією з ЛА. У зв'язку з цим пропонується новий принцип багатоканального обміну інформацією з ЛА завдяки використанню модернізованого частотно-часового методу вимірювання (МЧЧМВ) та підхід до синтезу перспективних ЛІВС.

Суть МЧЧМВ [3] полягає в тому, що із синхронізованого одномодового багаточастотного спектра випромінювання лазера за допомогою селектора подовжніх мод (СПМ) [4] виділяються необхідні моди (комбінації частот) для подальшого високоточного ВПР, автосупроводження та інформаційного взаємозв'язку з ЛА.

Запропонований СПМ, який забезпечує багаточастотне розділення каналів (багатоканальність), виконаний на основі вузькосмугових інтерферометрів Фабри–Перо, число яких дорівнює числу подовжніх мод, які селектуються, та містить в кожному з N каналів: оптичний поляризатор випромінювання, пасивну фазову пластинку $\lambda/4$, що повертає вектор Е минаючого випромінювання на кут 450 за один прохід, вузькосмуговий інтерферометр Фабри–Перо, налаштований на сигнал визначеної комбінації мод (частот), оптичний квантовий підсилювач, для підсилення вихідного випромінювання (виділення пари частот) і допоміжні дзеркала, призначені для каналізації оптичного випромінювання.

СПМ з багаточастотним розділенням каналів використовується в передавальній частці ЛІВС, за допомогою якого із синхронізованого одномодового багаточастотного спектра випромінювання YAG:Nd 3+ – лазера виділяються необхідні пари частот для створення:

інформаційного багатоканального зв'язку, за умови використання сигналу з різницевих частот міжмодових биттів

$\Delta\nu_{101}=\nu_{10}-\nu_1=9\Delta\nu_м$; … $\Delta\nu_{n2n1}=\nu_{n2}-\nu_{n1}=N\Delta\nu_м$;

рівносигнального напрямку на основі формування сумарної ДС завдяки таким чином, що частково перетинаються 4-х парціальні ДС, за умови використання різницевих частот міжмодових биттів

$\Delta\nu_{54}=\nu_5-\nu_4=\Delta\nu_м$, $\Delta\nu_{97}=\nu_9-\nu_7=2\Delta\nu_м$,

$\Delta\nu_{63}=\nu_6-\nu_3=3\Delta\nu_м$, $\Delta\nu_{82}=\nu_8-\nu_2=6\Delta\nu_м$.

Література: 1. Коломійцев О. В. Лазерна інформаційно-вимірювальна система // Зб. наук. пр. "Системи обробки інформації". – Харків: ХВУ, 2004. – Вип. 8(36). – С. 186 – 189. 2. Полігонні лазерні та оптико-електронні вимірювальні засоби: Конспект лекцій. Ч. II / С. В. Тюрін, І. С. Шостко, В. А. Романюк, В. В. Пономарьов, Р. В. Павлович. – Харків: ХВУ, 1998. – 174 с. 3. Деклараційний патент України на винахід 65099А, Україна, 6 МПК G01 S 17/42, G01 S 17/66. Модернізований частотно-часовий метод вимірювання параметрів руху літальних апаратів / Г. В Альошин, О. В. Коломійцев, Д. П. Пашков – № 2003054908; Заяв. 29.05.2003 // Бюлетень. – 15.03.2004. – № 3. – 8 с. 4. Коломійцев О. В. Селектор подовжніх мод для лазерної інформаційно-вимірювальної системи // Зб. наук. пр. "Системи обробки інформації". – Харків: ХУПС. – 2006. – Вип. 9(58). – С. 37 – 40.

УДК 339.187.42

Лебеденко М. С.

Е-БІЗНЕС ДЛЯ ДРУКОВАНИХ ЗМІ

Сьогодні кожне поважне іноземне видавництво давно має Web-сайт в Інтернеті. Друковані ЗМІ провідних країн світу, прагнучи йти у ногу з часом, формувати правильний імідж і розширювати читацьку аудиторію, в обов'язковому порядку створюють електронні версії своїх видань.

Таке масштабне заглиблення компаній у мережу дозволило значно розширити поняття "друкований медіа", який більше не обмежується паперовим носієм. У цьому руслі світові економічно сильні видання перетворюються зі звичайних видавців на постачальників різноманітного контенту (інформаційні агентства), який надалі розповсюджується читачами за всіма можливими каналами комунікації – телебачення, он-лайн, мобільні пристрої, папір, радіо тощо [1].

Яскравим прикладом цього можна назвати те, що в Європі за рівнем читання Інтернет уже давно наздогнав і, навіть, обійшов газети. Україні, на жаль, до цього ще далеко, проте ситуація розвивається у тому ж напрямку. Потроху, але вітчизняна галузь друкованих ЗМІ виходить за рамки традиційного бізнесу, збільшуючи оберти в електронному середовищі: зростають продажі реклами та інвестицій у пресу, розвивається поліграфія, впроваджуються передові медіатехнології.

У той же час український видавничий ринок залишається ще доволі молодим і має чимало проблем. Зокрема, отримання достовірних статистичних даних для проведення якісних маркетингових досліджень на цьому ринку ускладнюється цілим рядом факторів [2; 3]:

недосконалістю діючих інструментів державного статистичного спостереження за видавничою діяльністю;

відсутність галузевих механізмів саморегулювання для створення власного індустріального моніторингу статистичної інформації про видавничу діяльність;

нерозвиненістю системи тиражного аудиту та обліку реалізованих тиражів.

Окрім цього, активний розвиток індустрії періодичних друкованих ЗМІ гальмується непрозорістю та слабким механізмом систем підписного та роздрібного розповсюдження преси. Не сприяють покращенню ситуації й низький рівень контенту, велика кількість замовних матеріалів, часті порушення законодавства України у сфері реклами.

Спеціалісти переконані, що саме за цими чинниками криються основні причини скорочення інтересу до преси і відносно повільного зростання її рекламних доходів (що традиційно складають 2/3 усього прибутку фірми) порівняно з іншими ЗМІ.

Так, на фоні загального приросту рекламного ринку в цілому по країні ($1,8 млрд. у 2007 році) показники друкованих ЗМІ досить скромні, а їх приріст у грошовому еквіваленті збільшився з $176,8 млн. у 2006 році лише до $211 млн. у 2007 році [1].

Додамо, що в структурі вітчизняного рекламного ринку частка преси також менша, ніж частка телебачення, тоді як в європейських та інших розвинених країнах друковані ЗМІ утримують перше місце в загальному обсязі продажів. За даними компанії ZenithOptimedia у 2006 році на пресу припало 42% усієї світової реклами, тоді як на ТБ-рекламу – 37,8%, а на решту рекламних носіїв (Інтернет, радіо, зовнішню рекламу) – 20,2% [2].

З цього стає очевидним, що українські періодичні видання ще не оцінили усіх переваг електронних технологій. Для більшості з них, що вже існують у Світовій павутині, аудиторія сайтів – це аудиторія вже відомої однойменної паперової версії. Як можлива рекламна площадка такі Web-сайти почали розглядатися зовсім недавно – близько 3–5 років тому.

Проте, не дивлячись на певні прибутки від Інтернет-реклами, проекти поки не окупаються. Більше того, збиткові також спроби заробити на самому сайті, оскільки це відлякує цільову аудиторію. З іншого боку, ми маємо досвід зарубіжних країн, який демонструє явну прихильність рекламодавців саме до мережі. Так, на відміну від традиційної преси, заявлені тиражі якої значно перевищують реальні, кількість відвідувань Інтернет-ЗМІ об'єктивно відслідковуються різними лічильниками та внутрішньою серверною статистикою. Це, у свою чергу, також дозволяє визначити не лише кількісні, але й якісні показники аудиторії он-лайн-видання.

Таким чином, можемо зробити висновок, що поки вітчизняні друковані медіа лише починають рухатися у напрямку розширення своїх електронних версій до рамок рекламних площадок і їх єдина роль в житті компанії на сьогодні пов'язана з брендингом. За допомогою Інтернету формується лояльна аудиторія в тій частині користувачів, яка не має можливості купити аналогічну паперову версію. Одночасно це розширює знання марки, збільшує непрямі продажі текстів через партнерів, а також покращує індекс цитування, який формує постійний потік нових читачів, частина з яких надалі стає покупцями паперового видання.

Література: 1. Крапива С. Рекламобиоз // Бизнес. – 2007. – № 46. – С. 46 – 50. 2. Бжезинская М. Электронные версии печатных изданий: информация к размышлению // Интернет-газета "Главред" – 2007 // http://glavred.info. 3. Эксперты прогнозируют взрывной рост Интернет-рекламы в Украине // Интернет-газета "Экспрес-центр". – 2006 // http://www.expert.org.ua.

Левченко А. О.

УДК 621.396.6. 519.2

ВІДПОВІДНІСТЬ ХАРАКТЕРИСТИК ЕКСТРАПОЛЯЦІЙНОГО ФУНКЦІОНАЛА ПОХИБКАМ МОДЕЛЕЙ ФІЗИЧНИХ ПРОЦЕСІВ

Спроби впровадження в Збройних силах України обслуговування озброєння та військової техніки (ОВТ) за станом привели до погіршення стану озброєння та низки катастроф. Новим підходом до організації експлуатації складних технічних систем є реалізація положень теорії забезпечення експлуатації (ТЗЕ).

Забезпечення достовірності алгоритмів ТЗЕ пов'язано з вивченням помилок прогнозу стану ОВТ, обумовлених характером даних, неточностями моделей, обмеженістю і неоднорідністю інформації про реальні процеси.

Для атестації розрахункових процедур ММК [1; 2] вихідні використано дані Методики оцінювання незсувності й ефективності статистичних процедур Інституту технічної кібернетики АН УРСР ім. В. М. Глушкова, за якими оцінювалася завадостійкість алгоритмів структурної ідентифікації МГУА [3]. Визначення конкретних значень похибок ММК ідентифікації моделей проведено з ви-

користанням засад Методичних рекомендацій із метрологічної атестації алгоритмів статистичної обробки даних Науково-дослідного інституту метрології стандартизації та сертифікації ім. Д. І. Менделєєва. Цей вибір обумовлений з тим, що в Україні не існує нормативних актів у галузі атестації алгоритмів і програмних засобів.

Алгоритми ідентифікації ММК [4] містять процедури перевірки гіпотез про структуру моделі реального процесу. На пробних вибірках будуються варіанти характеристики положення моделі, які екстраполюються на відповідні контрольні вибірки. Сукупність отриманих екстраполяцій утворює екстраполяційний функціонал (ЕФ), щодо якого визначаються статистичні характеристики початкової вибірки. Це дозволяє інтерпретувати отриманий розподіл як оцінку випадкової похибки (ВП), а нев'язність ЕФ – як оцінку не виключеної систематичної похибки [4; 5]. Задача інтерпретації погрішностей моделі трансформується в початкову задачу математичної статистики. Специфіка цих задач полягає у відсутності інформації про характеристики випадкових чинників і в необхідності перевірки передумов застосування ймовірнісно-статистичних методів.

За відсутності інформації про характеристики випадкових чинників логіка статистичного виводу при перевірці гіпотез вироджується в перевірку відтворюваності статистичних характеристик моделей процесів. При оцінці ступеня адекватності моделей фізичних процесів експериментальним даним ММК оперує поняттям функції компактності [4] як міри стійкості моделей фізичних процесів еквівалентної характеристикам ВП моделі.

Отримав подальший розвиток підхід, який був запропонований ще у 1990 році [6]. Цей підхід вперше апробовано для алгоритмів, які реалізують розрахункові схеми ММК, методу найменших квадратів і методу найменших модулів [1; 2].

Таким чином, відповідність характеристик екстраполяційного функціонала похибкам моделей фізичних процесів вперше експериментально підтверджено [1; 2] не тільки для похибок вимірювань [4; 5], а й для похибок програмних засобів та моделей фізичних процесів.

Література: 1. Левченко А. О. Засоби атестації систем метрологічного супроводження // Матеріали 3-ї науково-технічної конференції "Стан і розвиток військово-морських сил Збройних сил України на сучасному етапі". – Севастополь, 2003. – С. 158 – 160. 2. Становський О. Л. Аналіз значень середніх модулів нев'язок і помилок екстраполяційних функціоналів моделей дрейфу / О. Л. Становський, А. О. Шевченко // Матеріали XI семінару "Моделювання в прикладних наукових дослідженнях". – Одеса: ОНПУ, 2004. – С. 5. 3. Ивахненко А. Г. Численное исследование помехоустойчивости многокритериальной селекции моделей / А. Г. Ивахненко, В. С. Степашко // Автоматика. – 1982. – № 4. – С. 26 – 36. 4. Блинов А. П. Обеспечение гарантированности решения задач вероятностно-статистическими методами / А. П. Блинов, С. Ф. Левин // Измерительная техника. – 1988. – № 12. – С. 8 – 10. 5. Левин С. Ф. Верификация экспертных систем, ориентированных на вероятностно-статистические методы в программах обеспечения эксплуатации аэрокосмической техники / Проблема разработки и внедрения экспертных систем. – М.: ВНИИМС, 1989. – С. 144 – 145. 6. Левин С. Ф. Сертификация программных средств статистической идентификации на заданной выборке / С. Ф. Левин, Д. А. Веретенин // Статистическая идентификация, прогнозирование и контроль РЭА. – Севастополь: Знание, 1990. – С. 32 – 35.

УДК 004.056.5:518

Нариманова Е. В.

ЭФФЕКТ ДВОЙНОГО КВАНТОВАНИЯ И ЕГО ИСПОЛЬЗОВАНИЕ ДЛЯ ДОКАЗАТЕЛЬСТВА ПОДЛИННОСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

Определение наличия фотомонтажа для изображения на сегодняшний день является актуальной проблемой с точки зрения защиты информации. Высокие темпы развития технических средств обработки и генерации цифрового изображения (ЦИ) и доступность программного обеспечения для его редактирования открывают широкие возможности для внесения несанкционированных изменений в ЦИ, а цифровым водяным знаком защищены далеко не все ЦИ.

Как правило, большинство современных ЦИ хранятся в формат JPEG с потерями, а большинство фальсификаций сводится к замещению некоторой области ЦИ на область другого ЦИ. После такого изменения полученное изображение сохраняется, как правило, снова в формате JPEG, что приводит к обязательному повторному квантованию коэффициентов дискретного коси-

---

нусного преобразования (ДКП) [1] измененного ЦИ. Один из наиболее распространенных методов, который используется для определения наличия фотомонтажа в ЦИ, основан на исследовании эффекта двойного квантования коэффициентов дискретного косинусного преобразования матрицы изображения [2 – 4].

В открытой печати на данный момент не были сформулированы достаточные условия проявления эффекта двойного квантования в виде периодически возникающих пиков и впадин на гистограмме коэффициентов ДКП дважды квантованного изображения. Целью данной работы является определение достаточного условия для проявления эффекта двойного квантования. Для этого необходимо установить соответствие между гистограммами коэффициентов ДКП матрицы ЦИ до первого и после второго квантования без восстановления и причину возникновения незаполненных столбцов в гистограмме коэффициентов ДКП матрицы ЦИ после второго квантования без восстановления.

Рассмотрим процесс изменения значений коэффициентов ДКП в процессе двойного квантования.

После первого квантования с восстановлением значение конкретного коэффициента ДКП u рассчитывается по формуле:

$$u^{(-1)} = [u / q^{(1)}]q^{(1)} = u^{(1)}q^{(1)},$$

где $u^{(-1)}$ – значение u после первого квантования с восстановлением;

$u^{(1)}$ – значение u после первого квантования без восстановления, $u^{(1)} \in Z$;

$q^{(1)}$ – соответствующий u коэффициент первого квантования, $q^{(1)} \in Z$,

$[\bullet]$ – операция округления аргумента до ближайшего целого.

После второго квантования без восстановления значение u рассчитывается по формуле:

$$u^{(2)} = \left[\frac{u^{(1)}q^{(1)}}{q^{(2)}} \right],$$

где $q^{(2)}$ – соответствующий u коэффициент второго квантования, $q^{(2)} \in Z$.

Пусть H и $H^{(2)}$ – гистограммы коэффициентов ДКП ЦИ, отвечающих выбранной произвольным образом частоте, до первого квантования и после второго квантования без восстановления соответственно. Введем функцию $n(u^{(2)})$ [2], которая определяет количество столбцов гистограммы H, внесших свой вклад в столбец $u^{(2)}$ гистограммы $H^{(2)}$.

В соответствии с источником [2]:

$$n(u^{(2)}) = q^{(1)} \left(\left\lfloor \frac{q^{(2)}}{q^{(1)}} \left(u^{(2)} + \frac{1}{2} \right) \right\rfloor - \left\lceil \frac{q^{(2)}}{q^{(1)}} \left(u^{(2)} - \frac{1}{2} \right) \right\rceil + 1 \right).$$

Функция $n(u^{(2)})$ имеет период $T = \dfrac{q^{(1)}}{НОД(q^{(1)}, q^{(2)})}$ [2].

Теорема. Для того чтобы гистограмма коэффициентов ДКП матрицы дважды квантованного изображения на периоде T имела нулевые значения, достаточно, чтобы второй шаг квантования был меньше первого, то есть чтобы выполнялось соотношение $\dfrac{q^{(2)}}{q^{(1)}} < 1$.

В данной работе сформулировано достаточное условие возникновения нулевых значений гистограммы коэффициентов ДКП матрицы дважды квантованного изображения. Цель работы достигнута. Результаты работы являются важными для создания математически обоснованного практического метода для определения и локализации фальсификации ЦИ, основанного на использовании эффекта двойного квантования.

Литература: 1. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес , Р. Вудс. – М.: Техносфера, 2005. – 1072 с. 2. He J., Lin Z., Wang L., Tang X. Detecting Doctored JPEG Images Via DCT Coefficient Analysis // ECCV. – №(3). – 2006. – 423 – 435. 3. Fridrich J., Goljan M., Du M. Invertible authentication // In SPIE, Security and Watermarking of Multimedia Contents. — 2001. 4. Popescu A. C., Farid H. Exposing digital forgeries by detecting traces of re-sampling // IEEE Trans. Signal Process. – 2005. – Vol. 53(2). – P. 758 – 767.

УДК 519:37

Огурцов В. В.

Пономарьова К. В.

МЕТОДИКА ОПТИМІЗАЦІЇ ІТ-ІНФРАСТРУКТУРИ ВНЗ НА ОСНОВІ ВІРТУАЛІЗАЦІЇ

У сучасних умовах стрімкого розвитку інформаційних технологій і як наслідок відчутного збільшення кількості різних програмних продуктів, комплексів і систем дуже складно встигати освоювати та адаптувати їх до освітньої діяльності. Але ж крім цієї проблеми багате розмаїття програмного забезпечення (ПЗ) породжує проблему ефективного управління (адміністрування, встановлення, інвентаризації) цим ПЗ, яке використовується в навчальному процесі. Для забезпечення якості освіти викладачі повинні мати можливість використовувати усе потрібне ПЗ у навчальному процесі. Але крім проблеми ефективного управління та ліцензування ПЗ постає проблема несумісності різних програмних продуктів, конфліктів, які вони можуть викликати в операційній системі.

Вирішувати ці проблеми потрібно у межах комплексної оптимізації ІТ-інфраструктури вищого навчального закладу. Проблемою оптимізації ІТ-інфраструктури організацій активно займаються такі гіганти ІТ-індустрії, як Microsoft [1], Sun Microsystems [2], IBM [3] та ін. Вагому частину в стратегіях оптимізації ІТ-інфраструктури організацій, які пропонують та розвивають ці компанії, займає віртуалізація. При цьому віртуалізація розвивається у різних напрямках: віртуалізація операційних систем, віртуалізація застосувань, апаратна віртуалізація, віртуалізація сховищ даних, віртуалізація представлень, віртуалізація мережі.

На перший погляд може здаватися, що усі переваги віртуалізації нівелюються значним підвищенням апаратних вимог. Але це не так або не так у разі коректного застосування віртуалізації. Тому розглянемо сутністю різних видів віртуалізації, їх переваги та недоліки.

Розглянемо детально варіант застосування віртуалізації в навчальному процесі у ВНЗ. На думку автора, насамперед значне спрощення управління ІТ-інфраструктурою навчального процесу забезпечить повсюдне (на кожній робочій станції, які використовуються в навчальному процесі) використання віртуальних машин. Найбільше спрощення та в той же час гнучкість забезпечить наступна схема управління ІТ-інфраструктурою навчального процесу: на кожній робочій станції в несистемному розділі в стандартному каталозі розміщуються образи віртуальних дисків зі встановленими операційними системами, які використовуються у навчальному процесі; ці операційні системи мають базову конфігурацію (без встановлення додаткового ПЗ, яке специфічне для якої-небудь дисципліни); повні права доступу до базових файлів образів повинні мати тільки адміністратори; викладачі та студенти повинні мати тільки права на копіювання та виконання (відкриття) цих файлів; на сервері у спільному каталозі викладачі заздалегідь за деякий час (залежно від кількості робочих станцій, які використовуються для викладання відповідної дисципліни), згідно з загальною політикою обчислювального центру, який обслуговує навчальні комп'ютерні класи, розміщують або оновлюють диференційні файли образи жорстких дисків (differencing virtual hard drive) базової конфігурації; в цих файлах образів ОС зберігаються лише зміни щодо базової віртуальної ОС, які відбуваються під час встановлення та конфігурування відповідним викладачем потрібного ПЗ для дисциплін(и), що він викладає; адміністратор здійснює копіювання відповідних диференційних файлів образів у каталоги на робочі станції, які відведено для відповідної дисципліни; при цьому доступ на читання до цих каталогів (на сервері з локальної мережі та на робочих станціях) також мають студенти; для виконання лабораторних робіт студент повинен створити у відповідному каталозі (для роботи у цьому каталозі він має необхідні права) віртуальну машину з диференційним віртуальним жорстким диском щодо віртуального диску відповідної дисципліни. Кожна хостова ОС повинна мати мінімальний типовий набір та конфігурацію встановленого програмного забезпечення, наприклад MS Office.

Ця схема дозволить з мінімальними витратами використовувати в навчальному процесі різні ОС, різне ПЗ та, зокрема:

адміністратору (обчислювальному центру, який обслуговує навчальні комп'ютерні класи): спростити процес управління (встановлення, адміністрування та видалення) ПЗ навчальних робочих станцій; значно посилити надійність та безпеку;

викладачеві: самостійно встановлювати та конфігурувати програмне середовище, як це найбільш потрібно для виконання лабораторних робіт за відповідної дисципліни; оперативно реагувати в межах навчального процесу на зміни в ІТ-сфері;

студентам: мати рівні умови навчання в комп'ютерних класах; мати можливість виконувати лабораторні завдання під час самостійної роботи (наприклад, вдома); відмінити дії і тільки ті дії, які вони зробили під час виконання лабораторної роботи, шляхом створення нового диференційного віртуального жорсткого диска щодо віртуального диска відповідної дисципліни.

Як недолік можна зазначити зростання апаратних вимог до робочих станцій і серверів. Але згідно з тенденцією помітного зростання потужностей комп'ютерів широкого використання та зниження їхньої вартості й відповідно ціни цей недолік стає все менш значущим.

Також проблемою стає управління ліцензіями на віртуальні ОС та віртуальне ПЗ. Але ця проблема може бути вирішена завдяки укладанню договорів з розробниками ОС та ПЗ, наприклад, як з Microsoft існує форма взаємодії, яка має назву MSDNAA (MSDN Academic Alliance), який дає право використовувати у навчальному процесі ВНЗ більшість з продуктів компанії, зокрема операційні системи, безкоштовно. Така тенденція посилення співпраці компаній розробників різного ПЗ прослідковується останнім часом. Звісно, це результат плідної співпраці як активних співробітників ВНЗ, так і компаній розробників ПЗ, які не менш зацікавлені в цій співпраці.

У підсумку можна відмітити важливість комплексної оптимізації IT-інфраструктури організацій і значну роль в неї концепції віртуалізації та зокрема використання цієї концепції у ВНЗ, що накладає свої особливості.

Література: 1. ИТ-инфраструктура / http://www.microsoft.com/rus/business/infrastructure/default.mspx 2. Эффективность ИТ-инфраструктуры: виртуализация на всех уровнях ИТ / http://www.pcweek.ru/white-papers /download.php?ID=104891 3. Оптимизация ИТ-инфраструктуры / http://www.ibm.com/ru /events /presentations /bf2007/

Пелевін С. Л.

УДК 004

МОДЕЛІ ТА МЕТОДИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Ефективне керування організацією, підприємством, галуззю − неможливе без прийняття виважених, аргументованих рішень. Прийняття таких рішень вимагає від керівників та аналітиків проведення аналізу великих обсягів інформації, як правило, в умовах істотних часових обмежень. Можливість аналізу даних припускає необхідність у проведенні збору вихідних даних та находженні у них різного роду закономірностей і тенденцій, найчастіше − прихованих. У зв'язку з цим великої актуальності на даний час набуває розробка моделей і методів, призначених для аналізу великих масивів даних із метою прийняття рішень.

Розглянуто наступні питання та результати досліджень:

узагальнена технологія проведення інтелектуального аналізу даних, аналіз її складових та етапів. Дослідження та принципи взаємодії компонентів Data Mining з компонентами OLAP [1; 2].

пропонуються для розгляду моделі та методи визначення ризику виникнення критичних ситуацій і процесів, що здійснюють негативний вплив на об'єкт (бізнес-сутність) [3; 4]. У рамках запропонованого методу здійснено модифікацію алгоритму кластеризації "k-середніх". У формалізованому вигляді задачу можливо представити наступним чином: існує певна кількість об'єктів $S_n^{R_i}$, які характеризуються певним набором параметрів $A_n^{S_i^{R_i}}$, що визначають як кількісні показники об'єкта, так і якісні показники. Оперуючи накопиченою історичною інформацією щодо об'єкта, можливо, оцінюючи поточні значення параметрів $A_n^{S_i^{R_i}}$, насамперед кількісних, визначити можливу майбутню зміну якісних показників вихідних об'єктів, тобто:

$$F(S_n^{R_n}(A_n^{S_n^{R_n}}), S'^{R_n}_n(A_n^{S_n^{R_n}})) = R(S_n^{R_n}(A'^{S_n^{R_n}}_n)),$$

де F() − методи обробки даних множин вихідних об'єктів, що застосовуються з метою отримання множини R;

$R(S_n^{R_n}(A_n^{S_n^{R_n}}))$ − результат вирішення задачі, що складається з підмножин вихідних об'єктів $S_n^{R_n}$ та прогнозованих значень якісних параметрів $A'^{S_n^{R_n}}_n$;

Пропонуються до розгляду моделі та методи оцінки можливих втрат прибутків підприємством в умовах ризику, результатами застосування яких є визначення оптимальних характеристик об'єктів, підготовка яких дозволить зменшити потенційні втрати при отриманні більших прибутків, враховуючи можливе виникнення критичного процесу Ei:

$$C(N, A_n^{S_n^{R_n}}), E(n, p) \to \max(B(N-n, V)) \cdot$$

Процес підготовки об'єкта в загальному випадку характеризується вартістю підготовки одного об'єкта C, кількістю підготовлених об'єктів N та параметрами об'єктів $A_n^{S_n^{R_n}}$. На процес підготовки об'єктів можуть впливати певні процеси (неочікувані ситуації) E_i, що не дозволяють здійснити їх наступний продаж, а, отже, ведуть до втрати прибутків. Процес E_i характеризується вірогідністю його виникнення p та кількістю знищених об'єктів n [5];

пропонується технологія розрахунку прогнозованих значень критичних показників об'єктів на основі кореляційно-регресійного аналізу [6].

Література: 1. Чубукова И. А. Data Mining. Учебное пособие. – М.: ИНТУИТ, 2006. – 382 с. 2. Bonczek R.H., Holsapple C., Whinston A.B. Foundations of Decision Support Systems. – New York: Academic Press, 1981. 3. Єріна А. М. Статистичне моделювання та прогнозування: Навч. посібник. – К.: КНЕУ, 2001. – 170 с. 4. Гитис Л. Х. Статистическая классификация и кластерный анализ. – М.: "Издательство МГТУ" , 2003 – 530 с. 5. Мармоза А. Т. Теорія статистики. – К.: Ельга, 2003. – 392 с. 6. Норман Дрейпер. Прикладной регрессионный анализ. Множественная регрессия / Норман Дрейпер, Гарри Смит. – Изд. 2-е. – К.: Диалектика, 2007. – 912 с.

УДК 621.37:621.391

Сорока Л. С.

Рассомахин С. Г.

МЕТОД ОБЕСПЕЧЕНИЯ СТЕГАНОГРАФИЧЕСКОЙ СКРЫТНОСТИ СИГНАЛЬНЫХ КОНСТРУКЦИЙ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Комплексная проблема обеспечения безопасности передачи данных в телекоммуникационных системах с открытой средой взаимодействия абонентов может успешно решаться только при использовании всех доступных средств защиты от несанкционированного доступа к конфиденциальной информации. Одним из важных направлений эффективной защиты является применение методов и технических средств стеганографических преобразований переносчиков информации на физическом и канальном уровнях протокола взаимодействия открытых систем. Это позволяет при общей доступности каналов телекоммуникационных систем обеспечить структурную скрытность систем модуляции и кодирования, которые в значительной мере снижают вероятность успешного вскрытия битового потока данных при анализе последовательностей сигналов перехватывающим объектом.

Следует отметить, что на фоне бурного развития стандартов криптографических преобразований и методов аутентификации, вопросы совершенствования структурной стеганографической скрытности физических переносчиков информации исследуются крайне недостаточно [1]. В то же время значение стеганографических преобразований чрезвычайно важно, особенно в системах временной стойкости, когда сочетание свойств простоты (дешевизны) и эффективности защиты данных приобретает первостепенное значение.

В основу рассматриваемого метода реализации сигнальных конструкций, защищенных от стандартных процедур демодуляции, положены способы обеспечения минимального объема сигналов при сохранении показателей частотно-энергетической эффективности переносчиков информации [2 − 5]. Теоретической основой метода является обобщение теоремы Котельникова для случая нерегулярного (локализованного) размещения отсчетных моментов при дискретизации огибающей сигналов на совокупности смежных интервалов модуляции [4]. Построение сигнальных конструкций осуществляется на основе ключевого базиса, содержащего относительные координаты отсчетных точек преобразования исходной модулированной последовательности на выбранном

временном интервале. Выбор базиса осуществляется по принципу равномерного распределения точек на совокупности исходных интервалов сигналов со стандартными видами дискретной модуляции, как правило, частотной или фазовой. Стойкость сигнальной конструкции к несанкционированной демодуляции определяется размером базиса, который, в свою очередь, при заданных параметрах спектра исходных сигналов связан с полной длительностью охватываемого интервала преобразования. Доступ перехватывающего приемника к битовому потоку данных при обеспечении приемлемого для дальнейшей обработки отношения сигнал/шум может быть достигнут только в случае отгадывания всех чисел базиса (количество которых может достигать нескольких сотен) при относительной ошибке, не превышающей 15 − 25 % для каждого из элементов. Вероятностный анализ метода обеспечения стеганографической скрытности показал, что применение даже простейших конструкций при ключевом базисе, содержащем 2 − 5 элементов, снижает общее количество информации, доступной перехватывающей стороне для дальнейшего криптоанализа, не менее чем в 2,5 − 3 раза.

Литература: 1. Столлингс В. Криптография и защита сетей: принципы и практика. – Пер. с англ.– 2-е изд. – М.: Изд. дом "Вильямс", 2001. – 672 с. 2. Уайнер А. Д. Фундаментальные пределы в теории информации // ТИИЭР. – Т. 69. – № 2. – 1981. − С. 117 – 132. 3. Сорока Л. С. Основы теории минимально-избыточных сигналов. Математические методы и средства обработки: Монография.– Харьков: МОУ, ОНИИ ВС, 2005. – 280 с. 4. Сорока Л. С. Сравнительная оценка эффективности применения минимально избыточных сигнальных конструкций для каналов связи с аддитивными гауссовыми помехами / Л. С. Сорока, С. Г. Рассомахин, В. И. Долгов // Зб. наук. пр. ОНДІ ЗС. – Харків: 2006. – Вип. 2(4). – С. 194 – 210. 5. Сорока Л. С. Применение полунепрерывных сигналов для интенсификации использования частотно-энергетического ресурса каналов передачи данных в АСУ / Л. С. Сорока, С. Г. Рассомахин // Інтегровані технології та енергозбереження. – Харьков: НТУ "ХПІ", 2007. – №3. – С. 121 – 124.

Ревак І. О.

Телефанко Н. Б.

УДК 004.056

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Нинішнє XXI століття знаменується вступом людської цивілізації в нову інформаційну епоху свого розвитку, що характеризується розгортанням новітньої інформаційно-телекомунікаційної революції, швидким поширенням інформаційних технологій, глобалізацією інформаційних процесів, а також появою інформаційних загроз і необхідністю забезпечення інформаційної національної безпеки.

Проблема підготовки фахівців у сфері захисту інформації є сьогодні однією з найактуальніших і найважливіших для всіх країн, що вступили і вступають в інформаційну епоху.

За кордоном сьогодні практично у всіх компаніях і фінансових установах є спеціальні служби з інформаційної безпеки, а в штатному розкладі − посади фахівців з інформаційної безпеки. У великих корпораціях і банках існують спеціальні посади, що відносяться до вищої управлінської ланки − це менеджер-адміністратор з інформаційної безпеки.

Головною метою будь-якої системи інформаційної безпеки є забезпечення стійкого функціонування об’єкта, запобігання загрозам його безпеки, захист законних інтересів користувача інформаційної системи від протиправних зазіхань, розголошення, втрати, витоку і знищення службової інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об’єкта [1].

Досягнення заданих цілей є можливим у ході вирішення наступних завдань:

1) віднесення інформації до категорії обмеженого доступу;

2) прогнозування і своєчасне виявлення загроз безпеки інформаційним ресурсам;

3) створення умов з найменшою ймовірністю реалізації загроз безпеки інформаційним ресурсам і нанесення різних видів збитку;

4) створення механізму й умов оперативного реагування на загрози інформаційній безпеці;

5) створення умов для максимально можливого відшкодування і локалізації збитку, що може бути нанесений діями фізичних і юридичних осіб, позбавлення негативного впливу наслідків порушення інформаційно-обчислювальної безпеки.

Цілком можливо, що найбільшою загрозою для обчислювальної системи є незадоволений службовець. Відомо багато випадків, коли один співробітник завдає істотних збитків. Звичайно, це відбувається випадково, як це було в системі резервування і замовлень квитків у системі однієї з авіаліній. Службовець системи частково зіпсував базу даних, підключаючи не ті магнітні носії. Іноді це робилось і навмисно, як, наприклад, у випадку з майором військово-повітряних сил, що знищив групу вхідних записів. Багато випадків продажу співробітниками секретної інформації і, поза сумнівом, набагато більша кількість подібних випадків не зареєстровані [2].

Якщо рівень моралі в організації низький, то підвищується загроза порушення безпеки. Деякі із співробітників виявляються вороже налаштованими і якщо їм випадає така можливість, свідомо шкодять. Інші готуються піти з організації. У сфері обчислювальної техніки відбувається частота зміни місць роботи. Деякі з тих, хто звільняється, можуть заздалегідь запастися цінною інформацією.

Зазвичай виправдовує себе поділ співробітників, що займаються розробкою і проектуванням, від тих, хто обслуговує і працює практично. Група, що займається розробкою, більше піддається впливу удачам і невдачам, раптовим змінам настроїв і бажань замовників. Для цієї групи більш імовірна наявність у її складі творчих, проте схильних до різного роду безладу працівників.

Помилки і провини окремих службовців, що не відносяться до категорії запланованих злочинів, мають місце частіше у тих організаціях, де панує низький рівень моралі службовців, там, де вони емоційно виснажені роботою. Для того, щоб мінімізувати імовірність таких явищ, керівник зобов'язаний знати кожного свого співробітника і бути в тісному контакті з ним. По можливості керівник повинен з розумінням ставитися до позаслужбової діяльності працюючих з ним службовців. Відсутність контакту зі співробітниками зазвичай стає помітною. Якщо лояльний службовець раптом виявляє ворожість щодо керівництва, розумний керівник буде, звичайно, попереджений і зможе вжити необхідних заходів для поліпшення морального стану співробітника або, якщо він зазнає невдачі, то переведе його на ту ділянку, де є менша ймовірність завдання збитків.

Відомо кілька випадків, коли програмісти при звільненні псували програми, або, що ще гірше, так їх модифікували, що при їхній реалізації мало місце перекручування даних. У літературі часто посилаються на випадок, коли звільнений програміст так модифікував програму розрахунку заробітної плати, що наступного дня під час виплати викликав страшний хаос. Якщо планується звільнення службовця на ділянці опрацювання даних, то він повинен негайно залишити своє робоче місце. Таким чином він буде позбавлений можливості вилити свій гнів на програми.

Якщо має місце тимчасове залучення працівників (що вкрай не бажано), чи службовців, їх варто ознайомити з вимогами режиму безпеки і зобов'язати суворо їх дотримуватися. Працівники, які залучаються до роботи ззовні, становить загрозу щодо режиму інформаційної безпеки. До цієї категорії працівників, звичайно, входять тимчасові секретарі, програмісти і консультанти. У ряді випадків вони мають можливість порушувати обмеження, встановлені для контактів між різними групами, отже, можуть бути завербовані для спроби проникнути в систему всередині організації або поза її межами. У тих сферах діяльності організації, які пов'язані з особливо важливими даними, наскільки це можливо, слід утримуватися від залучення сумісників чи тимчасових працівників [3, с. 418 – 419].

Службовці автоматизованої системи опрацювання даних повинні чітко і ясно усвідомлювати свою особисту відповідальність за забезпечення інформаційної безпеки. При переміщенні співробітника, що працював з несекретною інформацією, на нову ділянку, де йому доведеться знайомитись із закритими і секретними даними, необхідно дохідливо пояснити ту відповідальність, яка на нього покладається, а саме: порядок і правила збереження закритих даних; порядок розмноження, знищення, пересилання і внесення змін у секретні дані.

Даний співробітник повинен зрозуміти правила, що визначають усні обговорення секретних даних, з ним мають бути проведені бесіди про можливі спроби та методи проникнення до них, якими може скористатися порушник, окрім цього йому необхідно досконало вивчити спеціальні процедури підключення персонального комп'ютера до виконання секретних робіт.

Загалом, окрім вищезапропонованих заходів, необхідно також в обов'язковому порядку проводити роз'яснювально-виховну роботу, систематичні інструктажі та навчання правилам і засобам безпеки, регулярні, але несподівані тестування різних категорій співробітників із постійно поновлювальних програм та психологічних методик.

Література: 1. Дряшкаба Е. Т. Особливості оцінки безпеки інформаційно-обчислювальних систем // Захист інформації. – 2005. – №3. – С. 12 – 15. 2. Маракова И. И. Информационная безопасность комплексных систем связи / И. И. Маракова, А. А. Сыропятов // Захист інформації. – 2006. – №4. – С. 13 – 19. 3. Головко В. І. Фінансово-економічна діяльність підприємства: контроль, аналіз та безпека / В. І. Головко, А. В. Мінченко, В. М. Шарманська. – К.: Київський національний університет імені Тараса Шевченка, 2005. – 450 с.

Аллахверанов Р. Ю.

Хатнюк И. С.

УДК 681.7.068.4

ИССЛЕДОВАНИЕ СПОСОБОВ МИНИМИЗАЦИИ ОПТИЧЕСКИХ ПОТЕРЬ ПРИ СТЫКОВКЕ ОДНОМОДОВЫХ И МНОГОМОДОВЫХ ВОЛОКОН

Основной задачей при разработке конструкции и технологии изготовления оптических соединителей является снижение потерь. Для современного одномодового волокна достигнут коэффициент затухания, равный 0,2 – 0,5 дб/км, поэтому потери, вносимые соединителем, не должны превышать 0,17 – 0,25 дб.

Анализ влияния рассогласования на потери при стыке концов ОВ показывает, что конструкция соединителя и технология его изготовления должны обеспечивать весьма жесткие допуски. В конструкторско-технологических разработках для соединителей используются различные способы минимизации потерь [1].

Одним из направлений, реализующих минимизацию потерь, являются так называемые штекерные соединители, принцип действия которых преобладает в электронике, радиотехнике и технике проводной связи.

Оптическая деталь вследствие высокой хрупкости легко повреждается при сборке оптического прибора и поэтому нуждается в защитной оправе. Поскольку последняя изготовлена из металла и имеет цилиндрическую форму, она легко обрабатывается и открывает для конструктора широкий простор с точки зрения поиска вариантов ее сопряжения с другими деталями прибора, обеспечивающих его оптимальное функционирование.

Крепление волокна в прецизионно высверленном отверстии точно соосно со штекерным наконечником теоретически может обеспечить те жёсткие допуски, которые требуются для снижения потерь до требуемых. Однако для подобной обработки, по точности, лежащей на пределе возможностей современной техники, требуется уникальное оборудование и наивысшая квалификация исполнителя.

Погрешность, достигаемая на обычном оборудовании, ограничена следующими факторами: волокно после его вклеивания во внутренний канал наконечника оказывается несоосным с ним и имеет продольное смещение, которое существенно превосходит допустимое; торец волокна не попадает в плоскость переднего торца наконечника и имеет неровности; возникают перекосы конца волокна относительно осей наконечника.

Малые размеры наконечников и микроскопические размеры конца волокон делают вторичную обработку очень трудоемкой и требуют особого оборудования и высокой квалификации работников. Кроме того, добавляется кропотливая операция шлифовки и полировки его торца заподлицо с передним торцом наконечника. Эти операции (шлифовка и полировка) торца стекла являются крайне нежелательными, так как они нарушают структуру поверхностного слоя, ускоряя его коррозию. Поэтому обработанный торец волокна быстро мутнеет при длительном хранении.

При стыковке одномодовых волокон следует использовать прогрессивные конструктивно-технологические решения – с управляющими конструктивными и технологическими воздействиями, реализуемыми при изготовлении и эксплуатации соединителя.

Одним из подобных конструктивных принципов такого типа является самоюстировка волокон непосредственно в процессе микросборки.

В основу предлагаемого инновационного решения положен принцип юстировки стыкуемых волокон. Продольная юстировка (сведение двух концов волокон встык торцами без зазора) осуществляется при помощи конических ловителей волокна, изготовляемых в виде единой детали с зажимами концов волокна; вдвижение конца волокна в стыковочный канал и сближение его на заданное малое расстояние с торцом второго конца волокна контролируется ограничителем, зафиксированным вклейкой и опрессовкой на заданном расстоянии от торца первого волокна.

Основной задачей при выборе материала зажимов является минимизация модуля упругости для предотвращения сострогивания стружки острым краем торца волокна при его движении в ловителе. Наличие стружки не допускается, так как попав в зазор между стыкуемыми волокнами, она препятствует распространению света.

Из сказанного следует, что эффект юстировки может быть обеспечен только при изготовлении зажимов из высокополимерных органических материалов.

Первые конструктивные решения, основанные на самоюстировке, использовали клиновидные желобы в стыковочном устройстве.

Однако диаметр оболочки волокна имеет допуск, равный ±5мкм, при этом максимальный диаметр d_{max}= 130мкм, а минимальный d_{min} = 120мкм. Отсюда следует, что один торец стыкуемого

волокна в стыковочном клиновидном желобе может оказаться смещенным относительно другого не более, чем на 10 мкм, что недопустимо для одномодового волокна, у которого диаметр световедущего канала составляет 5–8 мкм. Использование нажима сверху посредством пуансона, накрывающего оба конца волокна с длинной стороной, не дает возможности совместить в вертикальной плоскости оси концов волокон. Последнее обусловлено западанием конца волокна с меньшим диаметром на более глубокий уровень, чем уровень залегания в клиновидном желобе конца волокна с большим диаметром.

Этого удается избежать, если канавку-желоб сделать цилиндрически симметричным в виде полого полуцилиндра. В этом случае нижние образующие цилиндрических концов волокон, размещенные в одной и той же вертикальной плоскости с их осями, при свободном размещении последних в круглом желобе расположены на одном и том же горизонтальном уровне.

Один из лучших вариантов прецизионной стыковки оптических волокон предполагает предварительное введение в желоб одного из концов волокон и его предварительную юстировку по горизонтальному вдвижению и предварительное закрепление дополнительным зажимом [2], расположенным за пределами основного зажимного устройства. Второй конец вводится после закрепления первого.

Введение обоих концов волокон упрощается, если желоб в пластине соединительного устройства к обоим концам этой пластины расширяется за пределами основного зажимного устройства: названные участки желоба играют роль нижних частей ловителей. После введения обоих волокон встык, осуществляется их зажим верхней пластиной, имеющей плоскую поверхность на участке основного зажимного устройства.

Юстировка состоит в том, что при погружении обоих концов стыкуемых волокон вместе с дном желоба и верхней пластины в упруго-податливый материал под действием нажима на оба конца в упруго-податливой верхней пластине накапливаются деформации и напряжения такие, что образующееся поле упругих напряжений приобретает минимальную энергию только в том случае, если оси концов стыкуемых волокон совпадают.

В результате теоретических и экспериментальных исследований предложено нетрадиционное для оптики конструкторско-технологическое решение, основанное на принципе самоюстировки, заключающемся в помещении концов стыкуемых волокон в цилиндрическую канавку зажимных пластин из эластомера [3]. Данное решение обеспечивает высокоточную юстировку стыкуемых волокон при обычных допусках на изготовление стыковочного узла, не требует высококвалифицированного персонала, специального оборудования и позволяет создать надежный соединитель невысокой себестоимости.

Литература: 1. Дмитриев В. К. Разъемные соединители для многоволоконных и жгутовых оптических кабелей //Приборы и техника эксперимента. – 1999. – №1. – С. 178 – 180. 2. Кабанов В. К. Методы изготовления оптических соединителей для волоконно-оптических линий связи / В. К. Кабанов, В. Ф. Кузнецов, С. П. Оробинский // Техника средств связи. Техника проводной связи. – 2000. – Вып. 12(57). – С. 87 – 90. 3. Заявка №2265110 /Франция/. Устройство для соединения светопроводящих волокон. - Заявл. 20.09.99; H 04 B 9/00.

УДК 004.056+330.341.1

Ревак І. О.

Зотова М. Є.

ІНФОРМАЦІЙНИЙ АСПЕКТ ІННОВАЦІЙНОЇ БЕЗПЕКИ

Сучасний світ переходить до інноваційної моделі розвитку. Більшість сучасних провідних країн розвиваються саме за рахунок впровадження і використання інновацій. Інноваційна модель розвитку економіки надійно підтверджую свою ефективність. Аналіз національних економік країн, що використовують таку модель, свідчить, що їх ефективність все меншою мірою визначається багатством природних ресурсів або дешевою робочою силою, і все більшою мірою − конкурентним використання знань і науковими нововведеннями.

Процеси глобалізації та геоекономічної конкуренції, що відбуваються в сучасному світі, зумовлюють нове ставлення та особливу увагу до питання інноваційного розвитку, без якого будь-яка країна приречена на неминуче відставання. Тому в кожній розвиненій країні велику увагу приділяють забезпеченню інноваційної безпеки.

Інноваційна безпека держави визначається спроможністю її науково-інноваційного потенціалу генерувати якісні зрушення в національній економіці, протистояти зовнішнім технологічним загрозам, гідно презентувати себе на світовому ринку технологій [1].

Нині спроможність до інновацій є однією з основ економічної безпеки держави. Якщо характеризувати зовнішній бік інноваційної безпеки, слід наголосити на забезпеченні науково-технологічної безпеки, тобто існуванні в країні потужного науково-інноваційного потенціалу, що дає змогу протистояти будь-якому диктату ззовні, пов'язаному з обмеженням доступу до передових технологій, розривом основних сформованих технологічних ланцюгів. Розвиток науково-інноваційного потенціалу має важливе значення для забезпечення обороноздатності країни. Внутрішня складова інноваційної безпеки пов'язана зі створенням, поширенням, впровадженням і використанням нововведень, що дають змогу запобігти стихійним лихам, катастрофам, терористам та іншим протиправним діям. З'являється також можливість протистояти використанню науково-технічних досягнень в антигромадських цілях.

Сьогодні в Україні існує декілька головних чинників-загроз інноваційній безпеці України: недостатній рівень фінансування науково-технічних робіт, слабкий розвиток інфраструктури трансферу технологій, зниження рівня "інтелектуалізації" експорту і зростання імпортозалежності країни від наукоємних товарів, недосконаліть податкової системи та відсутність державної підтримки цієї сфери, повільний розвиток ефективних форм інноваційної діяльності.

Однією з основних загроз є незадовільне інформаційне забезпечення інноваційної сфери, яке виступає важливим механізмом прискорення науково-технічного прогресу, а інформаційні ресурси – важливим елементом інтелектуальної власності. В умовах нової економіки важливим чинником економічного зростання є управління інтелектуальною власністю.

Інтелектуальна власність згідно із сучасними уявленнями є нематеріальним активом, використання якого у господарському обороті повинно перебувати у чітко визначеному правовому полі. Право володіння інтелектуальною (особливо промисловою) власністю є основою інноваційної діяльності, що дозволяє компаніям та винахідникам отримувати прибутки від інновацій. При цьому стан захисту інтелектуальної власності, патентної системи може стимулювати або стримувати цю діяльність.

Слід враховувати й нові можливості інтернаціоналізації інформаційного простору у забезпеченні технологічного розвитку. Нині у світі відбувається сплеск інформатизації бізнесу. Щоб підвищити свій імідж на глобальному ринку товарів і послуг, великі компанії створюють власні медіацентри, медіахолдинги і т. п. У розвинутих країнах широко використовують всі засоби інформації для освоєння науково-технічних досягнень інших країн та презентації власних переваг на світових ринках.

Значна частина отриманих в Україні наукових результатів не патентується, залишається не затребуваною, публікується у відкритих джерелах, передається за кордон безпосередньо науковими організаціями та недержавними структурами. Це, у свою чергу, дає можливість представникам іноземних держав практично безперешкодно використовувати українські розробки у своїх інтересах [2].

Утрата інтелектуальної власності відбувається через недосконалу правову та інформаційну захищеність інтелектуальної продукції вітчизняних авторів, а також через еміграцію наукових кадрів, що, безумовно, несприятливо відображається на впровадженні інновацій і новітніх технологій.

Основу інноваційної діяльності становить інформаційний елемент інноваційної інфраструктури в Україні – інформаційно-інноваційний центр і маркетингові компанії, які в комплексі забезпечують інформацію ринкового попиту і науково-технічні пропозиції [3].

Нинішнє суспільство проходить етапи процесу впровадження новітніх інформаційних технологій. Це забезпечує нову якість транскордонного інформаційного обміну і безпосередньо впливає на інноваційний розвиток кожної країни. Ось чому нині одним із основних засобів забезпечення державою своїх інтересів на міжнародній арені стає завоювання інформаційного простору шляхом розвитку інформаційних технологій та створення на їх основі інформаційних систем, котрі визначають доступ до досягнень у різноманітних галузях науки, техніки, економіки.

У сучасному світі здійснюється використання комп'ютерних мереж, відповідних потужним мультимедійним засобам, Internet, має місце глобалізація ефективних комунікацій, а це несе багато загроз інформаційного характеру. Так, через несанкціоноване проникнення до комп'ютерних баз даних багато технологічних і комерційних таємниць стають відомими третім особам, які використовують їх для власної вигоди.

Безумовно, інноваційна безпека значною мірою залежить від стану інформації безпеки України. Наша країна сьогодні не належним чином репрезентована в міжнародних інформаційних мережах, що не сприяє створенню позитивного іміджу держави, підприємств за кордоном, не дозволяє демонструвати їх потенціал та конкурентні переваги. Це пояснюється, насамперед, нерозвиненістю інформаційної інфраструктури, а саме телекомунікаційної системи країни.

З метою забезпечення захисту інноваційної безпеки необхідно вжити низку організаційно-технічних заходів:

підвищити рівень інформаційного забезпечення інноваційної сфери;

забезпечити використання додаткових заходів для збереження таємниць науково-технологічного характеру, фінансових і комерційних даних інноваційних проектів;

активізувати процес створення розвинутої національної інформаційної інфраструктури і входження у глобальну інформаційну інфраструктуру;

розробити методологічні та технічні напрацювання телекомунікаційних мереж, проводити періодичні тестування систем безпеки українських операторів зв'язку і комп'ютерних мереж. Так,

наприклад, Cisco Systems визначила кілька комплексних підходів, які об'єднані в стратегію інформаційної безпеки. Серед найновіших продуктів – послуги "Anti-X", призначені для запобігання мережним атакам, і послуги SSL VPN (Secure Sockets Layer Virtual Private Network). Окрім того, випущено набір додатків для управління безпекою – Cisco Security Management Suite [4];

забезпечити підготовку спеціалістів у сфері захисту інформації.

Література: 1. Сухоруков А. І. Проблеми інноваційної безпеки України // Стратегічна панорама. – 2002. – №5. – С. 75 – 81. 2. Ковальов Є. В. Інноваційний аспект економічної безпеки // Право і безпека. – 2005. – №2. – С. 169 – 171. 3. Федулова Л. І. Управління інноваційним розвитком регіону // Регіональна економіка. – 2005. – №2. – С. 37. 4. Каракай Ю. Без інноваційного розвитку немає майбутнього // www.rada.com.ua.

УДК 681.3

Шматко О. В.

Паніна М. В.

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ФОРМУВАННІ КОЛЕКТИВІВ

Сучасна психодіагностика надає практикуючим психологам широкий спектр методик, тестів і опитувальників для діагностування і прогнозу особових особливостей людини і дозволяє отримувати розгорнений психологічний висновок. Такі психологічні "портрети" можна використовувати для стимулювання особового зростання випробовуваних, а також для профілактики психологічних зривів і підвищення адаптивних властивостей людини.

Уявлення людини про саму себе й система її цінностей можуть бути виявлені за допомогою різних психологічних методів. Для створення адекватного психологічного випробовуваного "портрету" необхідно використовувати не один тест, а збалансовану систему тестів. Кількість тестів, використовуваних у конкретній роботі для психодіагностики, може бути різною [1].

Таким чином, наочна область психодіагностичної профорієнтації становить величезний інтерес для створення відповідних систем автоматизації. Слід зазначити, що інколи дуже важко оцінити стан і поведінку випробовуваних через відсутність кваліфікованих психологів. Тому доцільно в такі системи включати досвід провідних фахівців у цій сфері.

Тематика роботи є актуальною, оскільки формування виробничих колективів на високому науковому рівні неможливе без використання інформатизації процесів управління, широкого використання математичних моделей, нових інформаційних технологій.

Сучасні автоматизовані системи тестування нових співробітників не враховують особистісні якості респондентів, мають вузьку спрямованість і не характеризують особистість у цілому, тому актуальною є необхідність розробки нових моделей, алгоритмів і програмних продуктів, які б дозволяли формувати виробничі колективи за даними тестування, що враховує всі аспекти особистості [2].

Використання сучасної комп'ютерної техніки надає якісно нові можливості для проведення діагностики особистості й групи. Це можна віднести до всіх етапів процесу діагностики [2].

Використання комп'ютера в процесі оцінки кадрів дозволяє підвищити об'єктивність результатів обстеження, знизити вплив психолога (кадровика) на процес і підсумок тестування. Разом з тим, при цьому варто враховувати специфіку проведення комп'ютерної діагностики. З одного боку, вона пов'язана з організацією взаємодії психолога із програмними засобами, що реалізують тест на екрані монітора й наступних процедур його обробки та збереження результатів. З іншого боку – це особливості взаємодії людини, яка проходить тестування, як із власне комп'ютером (феномен "остраху комп'ютера"), так і з матеріалом тесту.

Особливістю систем психодіагностики персоналу є те, що в єдиній системі акумулюються результати декількох тестів. Розробка батареї тестів припускає декілька завдань [3]. В рамках першого завдання система повинна виконувати роботу із створення, редагування і супроводу БД (бази даних) випробовуваних, включаючи захист від несанкціонованого доступу до інформації. Друге завдання – управління викликом і функціонуванням окремих систем тестування.

Такі системи дозволять виконувати тестування й оцінку випробовуваних, а також давати необхідні поради та рекомендації практично на будь-якому підприємстві, де буде забезпечений доступ до Інтернет. Практично будь-який співробітник відділу по роботі з персоналом зможе проводити необхідні психодіагностичні дослідження, отримувати консультації фахівця, стежити за станом і психологічним "портретом" випробовуваних. Слід зазначити, що розвиток таких систем останнім часом привертає все ширше коло фахівців.

Література: 1. Беседин А. Н. Книга практического психолога. У 2 ч. / А. Н. Беседин, И. И. Липатов, А. В. Тимченко. – Харьков: Фортуна-прес, 1996. – 848 с. 2. Современный бизнес: Учеб. В. 2 т. Т. 1: Пер. с англ. / Д. Дж. Речмен, М. Х. Мескон, К. Л. Боуви, Дж. В. Тилл. – М.: Республика, 1995. – 1052 с. 3. Мельничук А. С. Современные системы психодиагностики / А. С. Мельничук, В. А. Сергеев //http:www.psycho.ru/articles/-modern_system.html 4. Гаврилов Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилов, В. Ф. Хорошевский. – СПб.: Питер, 2001. – 384 с.

Аллахверанов Р. Ю.

Хатнюк И. С.

УДК 681.7.068.4

ИССЛЕДОВАНИЕ КОНСТРУКТИВНО-ТЕХНОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК МАТЕРИАЛОВ, ПРИГОДНЫХ ДЛЯ САМОЮСТИРОВКИ УЗЛОВ ВОЛС

В работе приводятся результаты анализа высокополимерных материалов, удовлетворяющих требованиям стыковочных и самоюстировочных узлов ВОЛС. Обоснован выбор фторопласта-40, в наибольшей степени обеспечивающего эти требования.

Сформулируем основные требования, предъявляемые к материалу для изготовления деталей стыковочного устройства и самоюстировочного узла ВОЛС.

Для изготовления этих деталей, зажимающих симметрично по отношению к оси волокон, необходим материал, у которого модуль упругости значительно меньше, чем у материала волокон. Тогда стыкуемые волокна являются фактически жесткими деталями, симметрично сжатыми упругоподатливыми зажимами. При симметричной относительно оси конфигурации этих зажимов и усилий сжатия происходит самоюстировка (точнее их самоцентровка, относительно оси).

Вторым важным требованием является отсутствие холоднотекучести материала в диапазоне используемых усилий сжатия, стабильность поведения материала под нагрузкой во времени, устойчивость к внешним воздействиям и, в частности, радиационная стойкость.

При поступательном движении волокна и продольной стыковки его торца с предварительно установленным концом второго волокна, острый край скола первого волокна, упирающийся в поверхность податливого материала зажима, не должен соструживать с нее стружку, которая, попав между стыкуемыми торцами волокон, будет препятствовать прохождению света. Названное условие налагает ограничения на твердость, прочность и коэффициент трения материала. В то же время твердость материала должна быть существенно ниже твердости волокна, чтобы при сжатии зажимы не раздавили стеклянный сердечник волоконно-оптического кабеля.

Набором свойств, пригодных для конструктивной реализации самоцентрирующего зажимного узла, обладают высокополимерные органические материалы.

Пластическая масса − это композиция, состоящая из полимеров и различных добавок, где полимеры являются основной частью композиции.

Наличие в композиции двух химически разнородных компонентов обусловливает существенные изменения (обычно улучшение) физико-механических свойств материала, который в указанном случае называют композиционным материалом (композитом). Частным случаем подобных материалов являются так называемые слоистые пластики (стеклотекстолит, гетинакс).

Комплекс свойств, определяющих механическое поведение полимеров, в некоторых условиях эксплуатации или испытаний при воздействии на них внешних сил значительно шире, чем для металлических материалов.

К основным эксплуатационным физико-механическим свойствам полимеров относятся: усталостная прочность, удельная прочность, ударная вязкость, твердость, долговечность, ползучесть, параметр релаксации напряжений.

Одним из высокополимерных материалов, перспективных для конструирования соединителей, является фторопласт.

Для изделий из фторопласта-4, 4Д, 4М исходным сырьем является рыхлый волокнистый порошок. Предварительная формовка придает прессованным таблеткам, пруткам или кубикам форму с кажущейся плотностью 1,83 г/см^3 при Т= 23 – 25 С□Спекание проводят при 370±10 □С, при нагревании выше 390 □С выделяется фтор, поэтому необходима вытяжка.

Кристаллическая фракция размягчается при 327 □С (мелкие частицы). При 370 □С вязкость расплава равна 1011 П, то есть в 106 раз выше вязкости, необходимой для литья под давлением, а выше 415 □С наступает разложение с выделением фтора. В этом основная трудность, связанная с формованием изделий.

Технология формования заключается в следующем. При температуре 23–25 □С прессуются таблетки или образцы другой формы. Легкое слипание частиц обеспечивает сохранение формы. Волокнистость частиц делает необходимым тщательное разравнивание порошка, загруженного в пресс-форму. Объем загрузочной камеры в 5 раз больше, чем объем готового изделия. Давление при прессовании при 23–25 □С лежит не ниже 250 кгс/см^2. Скорость движения пуансона не должна превышать 6–7 см/мин. Обычно увеличивают давление в течение 5 мин, затем дают выдержку 1 мин; чем выше таблетка по высоте (в диапазоне до 2 см), тем медленнее опускается пуансон и дольше выдержка при давлении. Изготовленные таким образом и сохраняющие свою форму изделия спекают в печах с рециркуляцией воздуха, и вращающимся подом. Продолжительность спекания составляет 1 ч на каждые 3 мм толщины.

Фторопласт-40 имеет высокие механические свойства (прочность, отсутствие холоднотекучести), радиационно стоек. Допускает переработку в изделия всеми методами, применяемыми для переработки термопластов.

Характеризуется широким диапазоном рабочих температур от −100 С до +200 □С. Степень кристалличности изменяется от 40 % до 60 % в зависимости от температурного режима и времени протекания различных стадий переработки.

Материал выпускается в виде шести различных марок: тонкого легкосыпучего порошка, гранул и суспензии (водной и спиртовой).

Детали из высокополимерного материала изготовляют обычно в пределах 5–7 классов точности.

Допускаемая шероховатость поверхности элементов пресс-формы выбирается в пределах Ra—0,32 мкм по ГОСТ 2789-73. В тех же пределах должен находиться класс чистоты поверхности изделий при наличии высококачественного прессовочного материала и правильном режиме прессования.

Выбранный в качестве высокополимерного материала для самоцентрирующих зажимов фторопласт-40 имеет следующие свойства:

плотность, г/см^2 – 1,65 – 1,70;

разрушающие напряжения, Н/см^2 при растяжении – (2,7-5)х10^7, при статическом изгибе – (3,3-3,4)х10^7;

относительное удлинение при разрыве, % – 150–400;

модуль упругости, Н/см при сжатии (20□С)~7х10^8; при изгибе(20□С) ~(9-10)х10^8;

твердость по Бринеллю, Н/м ~ (5,8-6,3)х10^7.

Анализ физико-механических параметров высокополимерных материалов, пригодных для изготовления пластин зажимного устройства, показал, что необходимым сочетанием свойств обладает фторопласт-40.

В результате экспериментального исследования формовочных свойств фторопласта-40 определен технологический режим формовки пластин зажимного устройства.

Фторопласт-40, обладая малым коэффициентом трения, обеспечивает плавный заход ОВ в зажимное устройство без задиров и особых усилий, исключая тем самым возможное повреждение ОВ.

Фторопласт-40 в отличие от фторопласта-4 имеет остаточные деформации в пределах усилий, необходимых для самоюстировки.

Литература: 1. Воробьева Г. Я. Химическая стойкость полимерных материалов. – М.: Химия, 1991. – 296 с. 2. Пугачев А. К. Переработка фторопластов в изделия. Технология и оборудование / А. К. Пугачев, О. А. Росляков – Л.: Химия, 1997. – 169 с. 3. Козлов П. М. Применение полимерных материалов в конструкциях, работающих под нагрузкой. – М.: Химия, 1996. – 360 с.

Шостак А. В.

УДК 629.3.06

ОБ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ПРОСТЫХ ДЕЛИТЕЛЕЙ В КОМБИНИРОВАННОМ ТЕСТЕ ПРОСТОТЫ

В настоящее время в системах защиты информации широко применяются несимметричные криптографические преобразования, которые в качестве ключевых параметров используют простые числа. Актуальна проблема построения быстрого алгоритма формирования простых чисел, основным этапом которого является тест проверки простоты [1]. Наибольшее распространение находит комбинированный тест простоты, одним из этапов которого является деление тестируемого числа на простые числа [1].

Деление на простые числа преследует цель уменьшить мощность множества M(k) и, значит, повысить вероятность выбора простых чисел из множества M(k). M(k) – множество целых чисел не кратных первым k простым числам 2, 3, 5,..., p(k). Пусть числа множества M(k) и множества простых чисел Z не больше некоторого числа X. Мощности множеств M(k) и Z будут равны (с точностью до k) при $k=\pi(X^{1/2})=k'$, где $\pi(X^{1/2})$ – число простых чисел, не превосходящих $(X^{1/2})$ [2].

Эффект от последовательного деления на первые k простые числа оценим относительным количеством составных чисел, удаленных из множества целых чисел не превосходящих числа X – $E(k)=(X-||M(k)||-k)/(X-||Z||)$, где $||M||$, $||Z||$ – мощности соответствующих множеств. Очевидно, что $||M(k')||+k'=||Z||$ и $E(k')=1$. То есть после проведения деления на $\pi(X^{1/2})$ первые простые числа множества $||M(k')||$ будет состоять только из простых чисел. Достаточно просто вычислить величину $||M(1)||=f(1, X)=X-1-[X/2]+1$, где второе слагаемое учитывает, что число ‘1’ не принадлежит к простым числам; [X/2] – ближайшее не превосходящее X/2 целое, равное количеству чисел кратных 2 и не превосходящих X; четвертое слагаемое учитывает, что число ‘2’ является простым. Формула для вычисления $||M(2)||$ имеет вид:

$$||M(2)||=f(2, X)=X-1-[X/2]-[X/3]+2+[X/(2 \times 3)],$$

последнее слагаемое учитывает количество чисел одновременно делящихся на 2 и 3. Аналогичный, но более громоздкий, вид имеют и формулы для k>2.

Результаты экспериментальной оценки E(k) при X=6000 приведены в таблице. Отметим, что $\pi(6000)=783$, $\pi(6000^{1/2})=21$ [2].

Таблица

Оценка эффективности от использования простых делителей в комбинированном тесте простоты

Число делителей, k	Относительное число делителей, k/21	E(k)	Мощность множества $||M(k)||$	Относительное количество простых чисел в множестве M(k), $783/||M(k)||$
1	0.0476	0.5750	3000	0.2610
2	0.0952	0.7665	2001	0.3913
3	0.1429	0.8430	1602	0.4888
4	0.1905	0.8867	1374	0.5699
5	0.2381	0.9103	1251	0.6259
6	0.2857	0.9285	1156	0.6773
7	0.3333	0.9412	1090	0.7183
8	0.3810	0.9523	1032	0.7687
9	0.4286	0.9613	985	0.7949
10	0.4762	0.9684	948	0.8259
11	0.5238	0.9749	914	0.8567
12	0.5714	0.9799	888	0.8818
13	0.6190	0.9841	866	0.9042
14	0.6667	0.9881	845	0.9266
15	0.7143	0.9914	828	0.9457
16	0.7619	0.9942	813	0.9631
17	0.8095	0.9962	803	0.9751
18	0.8571	0.9977	795	0.9849
19	0.9048	0.9988	789	0.9924
20	0.9524	0.9996	785	0.9975
21	1.0	1.0	783	1.0

Третья строка таблицы показывает, что после деления на 14,29% первых простых делителей относительное количество удаленных составных чисел достигнет 84,3%, а величина $\pi(6000)/||M(3)||=0.4888$. Величину $\pi(X)/||M(k)||$ естественно использовать в качестве оценки вероятности выбора простого числа из множества M(k). Очевидно также, что приведенные относительные оценки эффекта от последовательного деления на первые k простые числа не претерпят существенных изменений и при X>6000.

Литература: 1. Качко Е. Г. Анализ вычислительной сложности алгоритмов тестирования на простоту чисел многократной точности / Е. Г. Качко, А. В. Свинарев, О. А. Мельникова //Радиоэлектроника и информатика. – 1998. – №1. – С. 44 – 47. 2. Бухштаб А. А. Теория чисел. – М.: Просвещение, 1966. – 384 с.

УДК 681.3

Шматко А. В.

Гусева Л. В.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПОДБОРА ПЕРСОНАЛА С ИСПОЛЬЗОВАНИЕМ СЕТИ КОХОНЕНА ДЛЯ СТАНДАРТИЗИРОВАННОГО МНОГОФАКТОРНОГО ИССЛЕДОВАНИЯ

Новые информационные технологии внедряются в разные отрасли современной деятельности человека. Конечный результат, сроки выполнения и качество продукции зависят от персонала, который выполняет те или другие функции на предприятии. При формировании производственного коллектива руководитель опирается на свой опыт и интуицию, а также оценивает производственный стаж и квалификацию. Вследствие этого в дальнейшем в производственных коллективах могут возникать конфликты, действия некоторых сотрудников могут быть несогласованными. Решение этой проблемы невозможно без использования современных информационных технологий. Такие технологии должны обеспечивать решение соответствующих задач, связанных с формированием коллективов, повышения производительности труда за счет уменьшения конфликтов в коллективах, возможность уменьшить расходы, которые связаны с переформированием коллективов разного уровня.

На сегодняшний день существует ряд методик, призванных решать подобные задачи, но наиболее востребованным и популярным является метод стандартизированного многофакторного исследования личности, или СМИЛ [1].

Для построения портрета личности используется десять базисных шкал. Множество этих шкал может быть расширено в виду множественности особенностей личности, однако эти десять являются оптимальными с точки зрения количества и качества. Их сочетания определяют склонность к видам деятельности.

Существует множество компьютерных версий метода, но с развитием вычислительных и психологических технологий возникают новые усовершенствования в системе СМИЛ.

Усовершенствованием самого метода СМИЛ является тест Люшера, использующий предпочтения цветов, который реализуется путём раскрашивания интерфейса программы.

Особенностью СМИЛ является то, что его методику используют при решении разных социальных проблем. Этому способствует наличие шкал достоверности и базисных шкал, число которых варьируется в пределах количества рассматриваемых параметров личности. В одном случае СМИЛ определяет профориентацию, в другом – стиль межличностного поведения, в третьем – тип реагирования на стресс, выраженность лидерских черт и многое другое. Из этого следует, что, применяя эту методику, можно создать модель общества, которая даёт возможность анализа поведения личностей, предугадывания возможных конфликтов, выявления подходов для их решения и так далее. Для этого необходимы конечные данные теста исследуемых людей, проведение оценки данных. Инструментом для решения задачи моделирования социальной группы являются искусственные нейронные сети (ИНС). Выбор ИНС в качестве инструмента для решения поставленной задачи объясняется тем, что нейросетевой подход особенно эффективен в задачах экспертной оценки, так как сочетает в себе способность компьютера к обработке чисел и способностью человека к обобщению и распознаванию.

Конечные данные СМИЛ представляют собой количество баллов по выявляемой психологической характеристике некоторого множества исследуемых людей. Цель анализа данных заключается в выявлении групп. Задача состоит в поиске личностей с подобными психологическими особенностями с последующим объединением их в группы. Для проведения анализа используется самообучающаяся сеть Кохонена [2], достоинством которой является то, что она учится понимать саму структуру данных. Она проводит разведочный анализ данных.

Использование данного подхода позволит расширить базу для применения метода СМИЛ и совершенствовать систему выводов, что позволит повысить эффективность оценки личностных особенностей человека.

Литература: 1. Руанет В. В. Нейросетевые технологии как средство организации образовательного процесса / В. В. Руанет, А. К. Хетагурова //ifets.ieee.org/russian/depository/v8_i4/html/4.html 2. Стандартизированный многофакторный метод исследования личности СМИЛ (модифицированный тест MMPI) //www.psylist.net/praktikum/smil.htm

Юхно И. А.

Юхно А. И.

УДК 681.3

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ "ОПЛАТА ОБУЧЕНИЯ"

Современный этап развития высшего образования предполагает наличие такой формы обучения, как контрактная. В связи с этим необходимо фиксировать реальную оплату за обучение. В промышленных прикладных пакетах, таких, как 1С бухгалтерия, Парус, Галактика не обнаружилось соответствующего модуля. Следовательно, для этих целей был разработан программный модуль для контроля оплаты за обучение. Программный комплекс реализован в клиент-серверной архитектуре. В качестве сервера выступает СУБД Oracle XE [1], которая распространяется по свободной лицензии. Характеристики СУБД Oracle XE следующие:

объем пользовательский данных – 4 Gb;

количество процессоров – 1;

объем ОЗУ – 1 Gb.

В качестве клиентской части использовался лицензионный Access 2003 [2], который в настоящее время входит в наиболее распространенный офисный пакет MS Office 2003.

Бизнес-логика обработки деталей оплаты была разработана на языке PL/SQL и Java. Для работы клиентской части использовались стандартные средства Access 2003. Созданная информационная система успешно эксплуатируется в течение 3-х лет в Харьковском отделении ИНЭМ и в филиалах – городах Торез и Шахтерск. Имеется возможность экспорта введенных данных в 1С - Бухгалтерия, который применятся на предприятии.

Входным документом является:

выписка банка по оплате. Предусмотрен как ручной ввод данных с твердых носителей, так и автоматический ввод из файла, получаемого из банка.

выходными документами являются:

текущая ведомость по оплате;

задолженность за выбранный период;

структура контингента по филиалам;

структура контингента по специальностям.

В результате внедрения системы достигнуто следующее:

повысилась оперативность получения соответствующей информации;

сократилась, приблизительно на 50%, трудоемкость обработки информации;

повысилось качество принимаемых решений.

Литература: 1. www.oracle.com 2. www.Microsoft.com

УДК 681.3

Яковишин К. Н.

МЕТОДЫ, ТЕХНОЛОГИЯ, ИНВЕСТИЦИОННЫЙ ПРОЕКТ ЗАЩИТЫ РЫНКОВ ОТ НЕКАЧЕСТВЕННЫХ ФАЛЬСИФИЦИРОВАННЫХ ТОВАРОВ

Значительная часть покупаемых на рынке товаров – это материальные объекты, а сам процесс покупки – это процесс идентификации товара и идентификации состояния товара. И здесь имеет место проблема: не всегда удается правильно опознать товар и его состояние, тем более во время скоротечных торговых операций. По этой причине мировой рынок (а Украина – не исключение) наводнен некачественным фальсификатом, удельный вес которого растет быстрыми темпами. Подделывают все: лекарства, акцизные марки, стартеры, продукты питания, деньги и т. д. Наносится ущерб здоровью и экономике.

Проблема надежной идентификации товара – это проблема достоверного автоматического установления подлинности идентификационных параметров товара в условиях реального времени выполнения торговых операций. Имеется в виду установление истинности кода производителя, кода товарной позиции, номера единицы товара, даты выпуска, срока годности и пр.

Есть основания считать, что решение проблемы надежной идентификации товаров и защиты рынков от некачественной продукции можно решить с помощью методов защиты информации, адаптированных для защиты материальных объектов, и для этого уже есть все необходимые научные, технические, экономические и правовые предпосылки.

Используемая сейчас технология идентификации (технология штрих-кодов – EAN) и новейшая, еще только внедряемая технология радиочастотных меток (GS1) проблему не решают. Проблему может решить встраивание в материальный объект информационной защиты, дополненное использованием адаптированных методов защиты информации.

Автором было установлено, что идентификация материальных объектов может осуществляться несколькими способами: в автономном режиме путем анализа целостности и аутентичности параметров информационной структуры объекта или дистанционно, путем сверки параметров информационной структуры идентифицируемого объекта с удаленной заведомо истинной копией информационной структуры этого объекта. Каждый из способов может использоваться самостоятельно или совместно для повышения надежности. Оба способа обеспечивают заданную степень вероятности ошибки идентификации (теоретически эта вероятность может быть сведена к нулю). Способы содержат ноу-хау и в настоящее время патентуются.

Для практической реализации указанных способов было сделано предложение налоговому ведомству (ДПА) Украины осуществить проект по внедрению электронного оборота акцизных марок, что может дать госбюджету около 1,3 млрд. гривен в год. Предложение было одобрено ведущими экспертами и руководством ведомства.

Логическим развитием методов надежной идентификации материальных объектов стала разработка новой технологии и основанного на ней пилотного инвестиционного проекта по защите товарных рынков от некачественной фальсифицированной продукции [1]. Проект составлен в формате книги электронных таблиц MS-Exel, в соответствии с международной методикой ЮНИДО.

Реализация проекта даст возможность не только защитить товарные рынки и покупателей современными методами, но также одновременно позволит снизить издержки на защиту товаров и, следовательно, снизить их цены. Унификация средств защиты, тары и упаковки товаров позволит надежно уберечь природу от бытовых отходов.

Остается надеяться, что изложенное выше привлечет внимание заинтересованных лиц и организаций.

Литература: 1. Разработка технологии надежной идентификации товаров и внедрение на рынке алкогольной продукции. – Свідоцтво про реєстрацію авторського права на науково-технічний витвір № 20028. – К.: Державний департамент інтелектуальної власності, 2007. – 8 с.

Зміст

Секція 1
Методи та технології безпеки інформаційних систем

Секція 2
Захист інформації в комп'ютерних системах

Секція 3
Інформаційні та телекомунікаційні системи в бізнесі

Довідка про авторів

Бутова Р. К. – ст. викладач ХНЕУ

Гаврилова А. А. – викладач ХНЕУ

Смірнов О. А. – канд. техн. наук, доцент Кіровоградського національного технічного університету

Доренський О. П. – аспірант Кіровоградського національного технічного університету

Єсаулов М. Ю. – ад'юнкт очної форми навчання Військового інституту телекомунікацій та інформатизації Національного технічного університету України "КПІ"

Носов В. В. – канд. техн. наук, професор Навчально-наукового інституту психології, менеджменту та інформаційних технологій ХНУВС

Манжай О. В. – викладач Навчально-наукового інституту психології, менеджменту та інформаційних технологій ХНУВС

Ковальчук В. Н. – аспірант Житомирського державного університету ім. І. Франка

Домарєв В. В. – канд. техн. наук, доцент, експерт з питань інформаційної безпеки

Дорохова Л. П. – канд. фарм. наук, доцент Національного фармацевтичного університету

Дорохов О. В. – канд. техн. наук, доцент ХНЕУ

Чєвардін В. Е. – канд. техн. наук, доцент НТУ "КПІ"

Сорокін І. А. – начальник відділення ОТ навчальної лабораторії кафедри Військового інституту телекомунікації та інформатизації НТУ "КПІ"

Гросфельд Ю. А. – ст. викладач Запорізького національного технічного університету

Андрущенко Д. М. – аспирант Запорожского национального технического университета

Козина Г. Л. – канд. физ.-мат. наук, доцент Запорожского национального технического университета

Кобозева А. А. – канд. физ.-мат. наук, доцент Одесского национального политехнического университета

Неласая А. В. – ст. преподаватель Запорожского национального технического университета

Трифонова Е. А. – аспирант Одесского национального политехнического университета

Степанов В. П. – канд. техн. наук, профессор ХНЭУ

Юхно И. А. – канд. физ.-мат. наук, доцент ХНЭУ

Белодед Н. И. – канд. техн. наук, профессор Академии управления при Президенте Республики Беларусь

Завиленская Т. П. – студент 2 курса Академии управления при Президенте Республики Беларусь

Петров А. А. – ассистент Восточноукраинского национального университета им. В. Даля

Астраханцев А. А. – канд. техн. наук, доцент ХНУРЭ

Бондарь И. В. – студент ХНУРЭ

Петровская Н. А. – студент 2 курса Академии управления при Президенте Республики Беларусь

Емельянов С. Л. – канд. техн. наук, доцент Одесской национальной юридической академии

Охрименко С. А. – докт. экон. наук, профессор, зав. лабораторией информационной безопасности Молдавской экономической академии

Зуєнко А. В. – студент 5 курсу Запорізького національного технічного університету

Говоров А. О. – асистент кафедри захисту інформації Запорізького національного технічного університету

Нікуліщев Г. І. – асистент кафедри захисту інформації Запорізького національного технічного університету

Kostyshyn S. – PhD student Ternopil State Ivan Pul'uj Technical University

Золотарьов В. А. – канд. техн. наук, доцент ХНУРЕ

Лисенко І. В. – канд. техн. наук, доцент Національного аерокосмічного університету ім. М. Є. Жуковського "ХАІ"

Кудінов В. А. – канд. фіз.-мат. наук, доцент, начальник кафедри спеціальної техніки Київського національного університету внутрішніх справ

Ziad S. – student KhNU named V. N. Karazin

Malyakina T. – superior teacher KhNU named of V. N. Karazin

Халімов Г. З. – канд. техн. наук, доцент ХНУРЕ

Сєвєрінов О. В. – канд. техн. наук, доцент ХНУРЕ

Лосєв М. Ю. – канд. техн. наук, доцент кафедри інформаційних систем ХНЕУ

Федорченко В. М. – канд. техн. наук, доцент ХНЕУ

Чекурда О. М. – курсант 3 курсу Військового інституту телекомунікацій та інформатизації НТУ "КПІ"

Шарапов В. Г. – аспірант Військового інституту телекомунікацій та інформатизації НТУ "КПІ"

Кравчук О. І. – заступник начальника науково-організаційного відділу Інституту Сухопутних військ ім. Петра Сагайдачного Національного університету "Львівська політехніка"

Берко А. Ю. – докторант національного університету "Львівська політехніка"

Тутунару С. А. – канд. физ.-мат. наук доцент Молдавской экономической академии

Склифос К. Ф. – инженер лаборатории информационной безопасности Молдавской экономической академии

Гавриш Т. В. – канд. техн. наук, доцент ХНУРЭ

Тюпич Е. В. – студент ХНУРЭ

Астраханцев А. А. – канд. техн. наук, доцент ХНУРЭ

Вакуленко В. С. – студент ХНУРЭ

Ткачов А. М. – канд. техн. наук, научный сотрудник Харьковского университета Воздушных Сил им. Ивана Кожедуба

Король О. Г. – преподаватель ХНЭУ

Долгов В. И. – докт. техн. наук, профессор ХНУРЭ

Ивонин Д. С. – студент ХНУРЭ

Носик А. М. – м.н.с. Метрологического центра военных эталонов ВС Украины

Качур Л. Н. – аспирант Кировоградского технического университета

Коваленко А. Н. – ст. инженер информационно-вычислительного центра Харьковского университета Воздушных Сил им. Ивана Кожедуба

Сай В. Н. – с.н.с. НИЛ научного центра Сумского государственного университета

Щербаков А. В. – канд. техн. наук, доцент ХНЭУ

Кузнецов А. А. – докт. техн. наук, с.н.с., начальник информационно-вычислительного центра Харьковского университета Воздушных Сил им. Ивана Кожедуба

Грабчак В. И. – начальник НИЛ научного центра Сумского государственного университета

Пасько И. В. – научный сотрудник Научного центра боевого применения ракетных войск и артиллерии Сумского государственного университета

Королев Р. В. – адъюнкт Харьковского университета Воздушных Сил им. Ивана Кожедуба

Марьяновський В. А. – аспірант Київського національного університету ім. Тараса Шевченка

Юштін К. Е. – канд. фіз.-мат. наук, доцент Київського національного університету ім. Тараса Шевченка

Кравець П. О. – канд. техн. наук, доцент Національного університету "Львівська політехніка"

Коломійцев О. В. – канд. техн. наук, с.н.с., провідний науковий співробітник науково-дослідного відділу наукового центру Повітряних Сил Харківського університету Повітряних Сил ім. Івана Кожедуба

Коваленко С. П. – канд. техн. наук, доцент Харківського університету Повітряних Сил ім. Івана Кожедуба

Лебеденко М. С. – аспірант НТУ "КПІ"

Левченко А. О. – канд. техн. наук, доцент, заступник начальника з наукової роботи Наукового центру Сухопутних військ Інституту Сухопутних військ ім. Петра Сагайдачного Національного університету "Львівська політехніка"

Огурцов В. В. – канд. екон. наук, доцент ХНЕУ

Пономарьова К. В. – викладач ХНЕУ

Пелевін С. Л. – аспірант Київського національного університету будівництва та архітектури

Ревак І. О. – канд. екон. наук, доцент Львівського державного університету внутрішніх справ

Телефанко Н. Б. – студент економічного факультету Львівського державного університету внутрішніх справ

Зотова М. Є. – студент економічного факультету Львівського державного університету внутрішніх справ

Шматко О. В. – канд. техн. наук, доцент кафедри ІТіСУ Університету громадянського захисту України

Паніна М. В. – магістр УЦЗУ Університету громадянського захисту України

Томашевский Б. П. – научный сотрудник Львовского института Сухопутных войск

Сергиенко Р. В. – ст. преподаватель Львовского института Сухопутных войск

Белоковаленко А. Л. – магистрант Львовского института Сухопутных войск

Приходько С. И. – канд. техн. наук, доцент, заведующий кафедрой транспортной связи УкрГАЖТ

Безверхая Г. С. – студент 5 курса УкрГАЖТ

Белецкий А. Я. – докт. техн. наук, профессор, зав. кафедрой радиоэлектроники Национального авиационного университета

Московченко И. В. – инженер факультета военной подготовки Национального технического университета "ХПИ"

Рыбина Т. А. – студент 2 курса Академии управления при Президенте Республики Беларусь

Белецкий А. А. – мл. научный сотрудник Национального авиационного университета

Семченко Д. А. – инженер Харьковского национального университета им. В. Н. Каразина

Замула А. А. – канд. техн. наук, доцент, профессор Харьковского национального университета им. В. Н. Каразина

Борисенко А. А. – докт. техн. наук, профессор, зав. кафедрой электроники и компьютерной техники Сумского государственного университета

Кулик И. А. – канд. техн. наук, доцент кафедры электроники и компьютерной техники Сумского государственного университета

Баранник В. В – докт. техн. наук, с. н. с. Харьковского университета Воздушных Сил им. Ивана Кожедуба

Карпенко С. В. – канд. техн. наук, доцент кафедры безопасности информационных технологий Национального авиационного университета (г. Киев)

Яковенко А. В. – начальник центра спецтехники научно-исследовательского института Министерства внутренних дел

Знахур С. В. – канд. экон. наук, доцент ХНЭУ

Мисюра О. Н. – канд. техн. наук, в.н.с. Харьковского университета Воздушных Сил им. Ивана Кожедуба

Кислов А. А. – студент 2 курса Академии управления при Президенте Республики Беларусь

Короткина Л. А. – студент 2 курса Академии управления при Президенте Республики Беларусь

Нариманова Е. В. – аспирант Одесского национального политехнического университет

Сорока Л. С. – докт. техн. наук, профессор, декан факультета компьютерных наук ХНУ им. В. Н. Каразина

Рассомахин С. Г. – канд. техн. наук, доцент, профессор кафедры безопасности информационных систем и технологий ХНУ им. В. Н. Каразина

Аллахверанов Р. Ю. – ассистент ХНУРЭ

Хатнюк И. С. – студент 4 курса ХНУРЭ

Шостак А. В. – канд. техн. наук, доцент Национального аэрокосмического университета им. Н. Е. Жуковского "Харьковский авиационный институт"

Гусева Л. В. – преподаватель кафедры ИТиСУ Университета гражданской защиты Украины

Юхно А. И. – студент ХНЭУ

Яковишин К. Н. – канд. техн. наук, доцент НАУ