Державний університет телекомунікацій
Київський національний університет імені Тараса Шевченка
Національний авіаційний університет
Військовий інститут телекомунікацій та інформатизації
Національний університет “Львівська політехніка”
Вінницький Національний технічний університет
Національна академія оборони України
Академія Служби безпеки України
Інститут спеціального зв’язку та захисту інформації
Університет Бульсько-Бяла
Вроцлавський технічний університет

ІІІ МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ НАУКИ І ТЕХНІКИ»

ЗБІРНИК ТЕЗ

19 травня 2016 року

м. Київ

State University of Telecommunications
Taras Shevchenko National University of Kyiv
National Aviation University
Military Institute of Telecommunications and Information
Lviv Polytechnic National University
Vinnytsia National Technical University
National Defence Academy of Ukraine
Academy of Security Service of Ukraine
Institute of Special Communication and Information Protection
University of Bielsko-Biala
Wrocław University of Technology

II INTERNATIONAL SCIENTIFIC-TECHNICAL CONFERENCE

«ACTUAL PROBLEMS OF SCIENCE AND TECHNOLOGY DEVELOPMENT»

BOOK OF ABSTRACTS

May 19, 2016

Kyiv

УДК 621.387:681.327

Актуальні проблеми розвитку науки і техніки: Матеріали третьої міжнародної науково-технічної конференції. Збірник тез. — Київ : ДУТ, 2016. — 33 с.

Даний збірник містить тези учасників конференції, представлених на III Науково-технічній конференції "Актуальні проблеми розвитку науки і техніки", яка проводилась 19 травня 2016 р. в Навчально-науковому інституті Захисту інформації Державного університету телекомунікацій, м. Київ.

Actual problems of science and technology: Proceedings of the third international scientific conference. Book of abstracts. - Kyiv: SUT, 2016. – 33 p.

This book contains abstracts of conference participants presented at III Scientific-technical conference «Actual problems of science and technology development », which was held on May 19, 2016 in the Educational-scientific Institute of Information security of the State University of Telecommunications, c. Kyiv

Робочі мови конференції - українська, російська, англійська.

Секретарі конференції

Складаний П.М. ст. викладач кафедри Інформаційної та кібернетичної безпеки, Дежравний університет телекомунікацій.

Платоненко А.В. асистент кафедри Систем захисту інформації, Дежравний університет телекомунікацій.

Рабчун Д.І. асистент кафедри Управління інформаційної безпекою, Дежравний університет телекомунікацій.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Програмний комітет:

ШЕВЧЕНКО Віктор Леонідович *(д.т.н., проф. , Київ, Україна);*
БУРЯЧОК Володимир Леонідович *(д.т.н., с.н.с., Київ, Україна);*
РОЗОРІНОВ Георгій Миколайович *(д.т.н., проф., Київ, Україна);*
НАКОНЕЧНИЙ Володимир Сергійович *(д.т.н., с.н.с., Київ, Україна);*
СКЛАДАННИЙ Павло Миколайович (*ст. викладач, Київ, Україна);*
ДРУЖИНІН Володимир Анатолійович*(д.т.н., проф., Київ, Україна);*
ОКСІЮК Олекесандр Глебович *(д.т.н., доцент, Київ, Україна);*
ТОЛЮПА Сергій Васильович *(д.т.н., проф., Київ, Україна);*
САМОХВАЛОВ Юрій Якович *(д.т.н., проф., Київ, Україна);*
ЮДІН Олександр Констянтинович *(д.т.н., проф., Київ, Україна);*
КОРЧЕНКО Олександр Григорович *(д.т.н., проф., Київ, Україна);*
КОЗЛОВСЬКИЙ Валерій Валерійович *(д.т.н., проф., Київ, Україна);*
СУБАЧ Ігор Юрійович *(д.т.н., доцент, Київ, Україна);*
ГОРБЕНКО Іван Дмитрович *(д.т.н., проф., Харків, Україна);*
ДУДИКЕВИЧ Валерій Богданович *(д.т.н., проф., Львів, Україна);*
НАЗАРКЕВИЧ Марія Андріївна *(д.т.н., проф., Львів, Україна);*
ГРИЩУК Руслан Валентинович *(д.т.н., с.н.с., .Житомир, Україна);*
БАЙЕР Анджей *(д.т.н., проф., Польща);*
ТУРМАНІДЗЕ Рауль Сергійович*(д.т.н., проф., Грузія);*
КАРПІНСЬКИЙ Микола *(д.т.н., проф., Польща);*
СУРМАЧ Томас (*PhD*, *Польща.)*

ЗМІСТ

С. О. Сєрих
к.т.н., доцент кафедри Інформаційних технологій
Державний університет телекомунікацій

НАПРЯМКИ ПІДВИЩЕННЯ СКРИТНІСТІ ПОВІДОМЛЕНЬ РАДІОМЕРЕЖ ІЗ СКЛАДНИМИ СИГНАЛАМИ

Низький рівень ефективності систем аутентифікації і авторизації радіоелектронного обладнання (РЕО) користувачів за рахунок спрощення програмного забезпечення, здешевлення кінцевих пристроїв та виключення спеціального обладнання захисту даних вказують на необхідність застосування особових дій для підвищення скритності обміну повідомленнями із застосуванням складних сигналів.

Для підвищення завадостійкості та конфіденційності РЕО доцільно використовувати складні сигнали із змінними параметрами, які завдяки своїм властивостям мають підвищену скритність, тобто маскують сам факт випромінювання, бо енергетично та структурно нагадують шум, тому мають назву [1] – шумоподібні сигнали (ШПС). Природно, що саме процес їх використання впливає на безпеку передачі даних, бо одночасно є додатком до змін в модуляції, кодуванні, спрощує реалізацію адаптації до рівня та виду завад, ускладнює розвідку параметрів і протидіє різноманітним видам загроз радіозасобам (РЗ).

Проведення аналізу видів скритності передавання повідомлень, факторів, що на неї впливають та визначення напрямків підвищення складна але актуальна задача. Для її розв'язання потрібен аналіз загроз для безпеки РЗ, який дозволить висунути вимоги до параметрів ШПС і визначити їх ефективність за властивостями. Розподіл загроз, як на найгірший випадок, диктується намірами систем протидії згідно прийнятих концепцій застосування [2] і поділяється на :

- порушення фізичної цілісності системи;
- перехоплення повідомлення, що передавалось;
- несанкціоноване проникнення в систему.

Їх аналіз вказує на доцільність підвищення таких [3] видів скритності сигналів РЗ із застосуванням ШПС, як:

- енергетична скритність радіосигналу та модулюючого ШПС;
- структурна скритність виду і параметрів ШПС;
- інформаційна скритність повідомлення завдяки сигналу ШПС;
- тимчасова і просторова скритності сигналів.

З метою уніфікації обладнання і забезпечення скритності пропонується застосування такого виду сигналу як ФМ ШПС-ППРЧ із змінними параметрами та структурою, який гарантовано забезпечить:

- ефективну протидію впливу навмисних завад, боротьбу із інтерференційними та взаємними завадами в СРЗ завдяки збільшенню значення $Б_с$ для складової ФМ ШПС;
- підвищену скритність сигналу завдяки збільшенню частотної невизначеності за рахунок перерозподілу $Б_с$ до складової ППРЧ;
- покращену електромагнітну сумісність засобів СРЗ за рахунок оптимізації параметрів ФМ ШПС-ППРЧ до умов функціонування.

Список використаних джерел

1. Варакин Л. Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин.-М.: Радио и связь, 1985.-384 с.

2. Серых С.А. К вопросу о влияниях радиоэлектронных помех на современные и перспективные радиоэлектронные системы связи/ Серых С.А., Соловьев В.Р., Богуш В.В. // ЗВ'ЯЗОК.— 2008.— № 2.- С. 69–73.

3. Сєрих С.О. Проблеми завадостійкості радіоліній з складними сигналами в умовах активних завад. // ЗВ'ЯЗОК.—2013.-- № 4.- С. 32-37.

Мушта С.С.
аспірант кафедри Вищої математики
Державний університет телекомунікацій
м. Київ, Україна

АНАЛІЗ САМООРГАНІЗУЮЧИХ МЕРЕЖ
SELF ORGANIZING NETWORKS

Саморганізуюча система (SON) - це набір процедур (чи функцій) для автоматичного налаштування, оптимізації, діагностики і ремонту стільникових мереж. Вона є необхідною для майбутніх мереж мобільного зв'язку та операцій в основному за рахунок можливої економії капітальних витрат та операційних витрати, представляючи SON. Сім'я самоорганізуючої системи складається з різноманітних функцій, які залежать від рівнів, на яких вони виконуються. Так як кількість функцій самоорганізуючих систем буде збільшуватися з кожним новим постачальником релізів, одним з головних питань для операторів буде, які функції ввести і визначити відповідний час для активації цих функцій, для забезпечення функціонування економічно ефективної мережі.

Основні переваги впровадження SON в стільникових:

(I)скорочення часу і витрат на установку;

(II) зменшення експлуатаційних витрат за рахунок скорочення ручної роботи в сукупності з системою моніторингу, оптимізації, діагностики, ремонту і мережі;

(III) скорочення капітальних витрат за рахунок більш оптимального використання мережних елементів;

(IV)поліпшення користувацького досвіду.

(V) підвищення продуктивності мережі.

Самооптимізація функцій SON, спрямована на забезпечення якості і продуктивності мережі при мінімумі ручного втручання оператора. Само-оптимізація функцій, контролює та аналізує дані про продуктивність і автоматично ініціює дії щодо оптимізації постраждалих мережевих елементів при необхідності. Це істотно знижує обсяг ручних операцій і замінює їх на автоматичні настройки збереження мережі. Самооптимізовані функції SON роблять можливим впровадження нових автоматизованих процесів, які занадто швидкі і/або занадто складні, щоб бути реалізовані вручну. Це дозволить підвищити продуктивність мережі, що робить мережу більш динамічною і адаптованою до мінливих умов трафіку і поліпшення користувацького досвіду.

Деякі з найбільш важливих випадків використання самооптимізації SON включають:

(I) фізичний ідентифікатора стільника;

(II) Інтер-стільникове втручання координації;

(III) мобільність, надійність оптимізація;

(IV) мобільність балансування навантаження, оптимізація.

Перші два приклади використання, можуть також бути класифіковані як самостійні конфігурації алгоритмів, так як вони будуть частиною початкової конфігурації процедур, але також відіграють важливу роль у нормальній діяльності і може розглядатися в якості самостійної оптимізації процедур.

Майданнік М. К., Борисенко А.В.
студентки кафедри Управління інформаційною безпекою
Державний університет телекомунікацій
м. Київ, Україна

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

В умовах підвищення рівня внутрішніх і зовнішніх загроз інформаційної безпеки, безпосередньо впливаючих на фінансову діяльність підприємства і його стійкість на ринку, захист інформаційних ресурсів є одним з ключових завдань підприємства. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. В сучасних умовах, без належного захисту інформаційного середовища підприємства не можливо забезпечити його економічну безпеку.

Для реалізації політик ІБ у державному секторі, де існують певні законодавчі вимоги, застосовується Комплексна система захисту інформації (КСЗІ).

У випадку окремих суб'єктів, що реалізовують захист своїх інформаційних ресурсів на власний розсуд, можуть бути застосовані міжнародні стандарти ISO: ISO/IEC 27002:2013, ISO/IEC 27001:2013 та ін. — для підтримки рішень на основі ITIL та COBIT. Тоді на підприємстві створюється Система управління інформаційною безпекою (СУІБ).

Однією з основних умов ефективного функціонування системи управління ІБ є залученість керівництва компанії в процес управління ІБ.

Основна складність може полягати в перевірці ефективності процедур СУІБ. Тобто для кожної процедури необхідно розробити критерії, за якими буде перевірятися її ефективність, і, крім цього, такі критерії потрібно розробити для всієї системи управління в цілому.

Критеріями оцінки ефективності СУІБ можуть бути, наприклад, зміна кількості інцидентів ІБ, кваліфікація користувачів в області ІБ, досягнення поставлених бізнес-цілей [1].

Аналізуючи міжнародні стандарти серії ISO 27k та сучасні вимоги до організації ІБ на підприємстві можна дійти висновку, що впроваджені в Україні галузеві стандарти [2, 3] значно застаріли і не можуть бути достатньою базою для забезпечення комплексного захисту інформаційних активів підприємства.

Література:

1. ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing, 2011
2. ГСТУ СУІБ 1.0/ISO/IES 27001:2010 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги"
3. ГСТУ СУІБ 2.0/ISO/IES 27002:2010 "Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою"

Тарасенко Н. А.
студент кафедри Управління інформаційною безпекою
Державний університет телекомунікацій
м. Київ, Україна

ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Документована політика ІБ повинна встановлювати підхід до управління інформаційною безпекою, визначати поняття інформаційної безпеки, її основні цілі та область дії, містити основні положення для визначення цілей і механізмів контролю, включаючи структуру оцінки і управління ризиками [1].

При цьому слід пам’ятати, що цільова аудиторія політики ІБ - кінцеві користувачі і топ-менеджмент компанії, які не розуміють складних технічних виразів, проте повинні бути ознайомлені з положеннями політики.

Аналіз досвіду формування політик ІБ у сусідніх країнах, та країнах Європи, свідчить, що керівники підприємств досі не до кінця розуміють призначення цього документу, перенасичують його технічними термінами і необгрунтовано роздувають його об’єм.

Адекватний рівень інформаційної безпеки в сучасній організації може бути забезпечений лише на основі комплексного підходу до написання і впровадження політики ІБ.

За результатами дослідження вироблено наступні рекомендації по підвищенню ефективності формування політики ІБ підприємства:

- Предмет політики. Відповідальний спеціаліст повинен повністю визначити область її застосування за допомогою обмежень і умов у зрозумілих усім термінах. Також необхідно явно вказати мету або причини розробки політики.
- Застосовність. При написанні політики необхідно уточнити де, як, коли, ким і до чого застосовується дана політика.
- Ролі та обов'язки. Потрібно описати відповідальних посадових осіб і їх обов'язки щодо розробки та впровадження різних аспектів політики.
- Дотримання політики. Для деяких видів політик може виявитися доречним опис, з деяким ступенем детальності, порушень, які є неприйнятними і наслідків такої поведінки.

Література:

1. ISO/IEC 27001:2013 information technology — security techniques — information security management systems — requirements, 2013.
2. ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls, 2013.

Арделян В.В.
аспірант кафедри льотної експлуатації, аеродинаміки та динаміки польоту
Кіровоградська льотна академія Національного авіаційного університету, м. Кіровоград, Україна
Мусієнко А.П.
доцент кафедри вищої математики
Державного університету телекомунікацій, м. Київ, Україна

ОСНОВНІ ЕТАПИ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ПІЛОТАЖНО-НАВІГАЦІЙНОГО КОМПЛЕКСУ ПОВІТРЯНОГО СУДНА

В даній доповіді буде розглянута основна ідея забезпечення функціональної стійкості пілотажно-навігаційного комплексу (ПНК) повітряного судна (ПС). Ця ідею полягає в тому, що необхідно постійно мати інформацією про достовірність елементів бази знань, на основі якої побудовано систему підтримки прийняття рішень ПНК ПС. Знання, як відомо, мають суб'єктивний характер, а їх істинність росте в процесі накопичення досвіду. В подальшому цю інформацію використовувати при формуванні відновлюючого управління, яке парирує наслідки позаштатних ситуацій.

Запропонована ідея забезпечення в ПНК повітряного судна властивості функціональної стійкості, складається з наступних етапів:

1. *Етап виявлення*, який полягає у виявленні факту появи позаштатної ситуації. Залежить в основному від ступеня виразності так званого приваблюючого ефекту. При добре вираженому приваблюючому ефекті ситуація відразу звертає на себе увагу. Нештатні ситуації із середнім приваблюючим ефектом виявляються, як правило, шляхом порівняння заданих параметрів, що характеризують рух і текучих параметрів. Нештатні ситуації з низьким приваблюючим ефектом виявляються тільки шляхом порівняння стану декількох вимірювальних, обчислювальних, виконавчих систем.

2. *Етап розпізнавання*, який полягає в конкретизації та класифікації позаштатної ситуації. Дослідження різних варіантів побудови систем діагностування розподілених баз знань (РБЗ) дозволяють зробити висновок про те, що найбільш доцільною є організація тестового діагностування за принципом блукаючого діагностичного ядра. Динамічна децентралізована діагностування БЗ полягає в наступному. Елементарні перевірки окремих модулів БЗ з боку інших модулів виконуються у випадкові моменти часу. Обмін діагностичною інформацією про структуру діагностичних зв'язків і результати перевірок проводиться між модулями на основі способу умовної передачі результатів елементарних перевірок. Кожен модуль, отримуючи діагностичну інформацію, формує ознаку достатності для проведення алгоритму дешифрування отриманої інформації діагностування. Як ознака достатності використовується ймовірність видачі результату на основі отриманої множини результатів елементарних перевірок. При відповідності вказаної ознаки оптимальному значенню, модуль БЗ виконує алгоритм дешифрування інформації діагностування і визначення семантичного стану всіх модулів БЗ, а також між модульних зв'язків розподіленої бази знань.

3. *Етап відновлюючого управління*, який полягає в створенні управлінських впливів для локалізації та нейтралізації позаштатної ситуації. При цьому допускається реструктуризація та деградація ПНК.

В доповіді розкривається зміст вищезазначених етапів та ставляться завдання щодо розробки науково-методичного апарату забезпечення функціональної стійкості ПНК повітряного судна.

Кривульський Денис Святославович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

ОСОБЛИВОСТІ ЗАХИСТУ ВІД КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Відповідно до законодавства України до комп’ютерних злочинів відносяться [1]:

- Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), що призвело до порушення властивостей інформації, а саме конфіденційності, цілісності або доступності. Окремим пунктом зазначені інсайдери, тобто особи, що мають певний доступ до інформації в системі, але при цьому виконують дії, що не санкціоновані їх службовим становищем.
- Створення, а також розповсюдження, або збут шкідливих програмних чи технічних засобів.
- Несанкціоновані збут, або розповсюдження інформації з обмеженим доступом.
- Умисне порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), методами атак відмови в обслуговуванні (DoS).

Основною особливістю захисту від комп’ютерних злочинів є цілковите покладання цієї сфери інформаційної безпеки на методи розслідування інцидентів та емпіричний досвід захисту від реальних атак. Оскільки комп'ютерні злочини зазвичай мають характер таргетованих атак і є найближчою точкою контакту між зловмисником і спеціалістами з інформаційної безпеки, захист інформаційних систем в цій сфері перш за все повинен бути динамічним.

Іншою значною особливістю є відсутність достатніх статистичних та фактичних даних про більшу частину інцидентів, оскільки компанії, що піддаються таким атак не зацікавлені у їх публічному висвітленні в зв’язку з репутаційними ризиками. Тому основними джерелами інформації для дослідження специфіки захисту від комп’ютерних злочинів є звіти крупних розробників захисного програмного забезпечення, наприклад Symantec [2], або Kaspersky Lab [3].

Типовий сценарій розслідування комп’ютерних злочинів:

- встановити джерело загрози - внутрішнє чи зовнішнє;
- з'ясувати сценарій атаки;
- визначити наслідки - скомпрометовані акаунти і системи;
- визначити подальші дії для ліквідації загрози.

Для забезпечення перших трьох етапів критичним є наявність в атакованій організації системи збору та аналізу журналів подій (логів). Необхідно правильно налаштувати сповіщення антивірусу IDS, DLP і інших систем безпеки, а також перевірити адекватність реагування систем захисту шляхом імітації реальних атак. Особливу увагу потрібно приділити точкам дотику із зовнішньою мережею і місцям зберігання чутливої інформації.

В процесі дослідження було з’ясовано, що для забезпечення комплексного захисту інформаційних систем від комп’ютерних злочинів найбільш критичними є наступні питання:

- Наявність системи менеджменту і аналізу журналів подій (логів).
- Наявність адекватних парольних політик, вимог до складності паролю та умов їх експлуатації, наприклад частоти оновлення.
- Наявність політики оновлення всього активного програмного забезпечення, включаючи менеджмент патчів безпеки.
- Наявність єдиної уніфікованої політики доступу до мережі, чітких і аргументованих правил розмежування мережевих ресурсів.
- Забезпечення сегментованості мережі та інкапсуляції мережевих ресурсів з загальним доступом.

Перелік використаної літератури:

1. Кримінальний кодекс України. Розділ XVI, Статті 361 – 363.
2. 2016 Internet Security Threat Report (ISTR)
3. Kaspersky Security Bulletin 2015. Overall statistics for 2015

І.В. Саламатін
Державний університет телекомунікацій

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ ПРИ РОБОТІ З ЕЛЕКТРОННИМИ ГРОШИМА

У сучасних умовах ведення бізнесу найважливіше місце в усіх сферах економіки, безумовно, посідає інформація. Тому особливу увагу слід приділяти її безпеці − захищеності інформації та інфраструктурі, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації. Під час роботи з грошовими коштами інформаційна безпека відіграє вирішальну роль у добробуті суспільства й фінансовій безпеці окремих економічних суб'єктів та дер- жави в цілому. При цьому фінансовій безпеці банку сучасні науковці надають такі характеристики:

-забезпечується рівноважний і стійкий фінансовий стан банку;

-вона сприяє ефективній діяльності банку;

-є можливість на ранніх стадіях визначати проблеми і уникати чи ліквідовувати їх;

-нейтралізуються кризи та запобігається банкрутство.

Питанням фінансової та економічної безпеки суб'єктів господарюван- ня та держави присвячені праці вітчизняних (Барановського О. І., Єпіфанова А. О.) та зарубіжних науковців. Питанням інформаційної безпеки присвячені публікації Берко А. Ю., Зими А. М., Карасюка В. В., Мясіщева О. А., Олексюка О. С., Рішняк І. В., Судейко М. А., Трубіна І. О. тощо. Однак питанням аудиту інформаційної безпеки, захищеності банків під час роботи з електронними грошима присвячена недостатня увага науковців.

Проводячи аудит інформаційної безпеки банку при роботі з електронними грошима, здійснюючи перевірку організаційно-технічної та правової готовності установи до роботи із даним платіжним засобом, аудиторам слід приділяти увагу, зокрема, підготовці персоналу банку, відповідального за інформаційну безпеку, організації доступів до елементів інформаційної системи, обмеженням програмно-апаратного доступу до інформаційної системи тощо.

Проводячи аналіз організаційних заходів, спрямованих на захист інформації, аудиторам доцільно приділити увагу наявності та якості документів, що регламентують емісію, обіг та погашення електронних грошей. Крім того, банкам-емітентам слід розробити ґрунтовні та докладні інструкції для користувачів щодо роботи з електронними грошима. У таких документах слід з'ясувати наявність рекомендацій, зокрема, щодо:

-обмеження довжини, складності та часу життя паролів, які забезпечують доступ до електронних гаманців чи інших елементів інформаційної системи;

-доцільності в тому, щоб пароль був відомий лише одному користувачеві.

У разі інциденту винен буде власник облікового запису, тому що відсутні докази, що це зробив не він, про що буде зафіксовано в протоколах дій співробітників, які є підтвердженням будь-яких дій в інформаційних системах.

Проводячи аудит інформаційної безпеки банку, який є учасником систем електронних грошей, необхідно звертати увагу не лише на традиційні організаційні й тех- нічні заходи, а й на психологічну підготовленість працівників до методів соціальної інженерії. Такий підхід до проведення сучасного аудиту в банку дозволятиме забезпечити інформаційну безпеку на належному рівні в умовах стрімкого розвитку технологій та ґрунтовного підходу до категорії «інформаційна система», яка є значно ширшою, ніж, наприклад, комп'ютерна, фінансова чи економічна безпека та і вимагає особливої підготовки аудиторів і залучення експертів до проведення перевірок. Аудит інформаційної безпеки банку під час роботи з електронними грошима − це не інструмент перевірки чи контролю, а засіб надання впевненості користувачам у тому, що система є надійною, безпечною та не створить фінансової та соціальної напруженості в суспільстві.

Деркаченко Я. А.
студент кафедри Управління інформаційною безпекою
Державний університет телекомунікацій

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ РІВНЯ ІНФОРМУВАННЯ СУСПІЛЬСТВА ПРО ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Кожна країна постійно перебуває під зовнішнім та внутрішнім впливом. Це проявляється у спробах встановити контроль над засобами комунікації та масової інформації. Метою цього є - маніпулювання громадською думкою в інтересах, які нерідко суперечать національним.

На сьогодні, механізми захисту свідомості особистості, соціальних груп та населення розроблені доволі слабо, а органи, які повинні контролювати ресурси можливого впливу, показують свою неспроможність протидіяти зазначеним загрозам в першу чергу через нескоординованість дій та відсутність єдиного органу управління. Нормативно-правова база України має значні прогалини і не побудована так, аби повноцінно сприяти швидкій і безперебійній роботі компетентних органів. Відсутність повноцінних власних інформаційних ресурсів, несе загрозу небезпечних впливів зацікавлених країн на свідомість громадян щодо тверезого вирішення окремих завдань.

Спеціальні інформаційні операції (СІО) - це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, з метою схилення до прийняття управлінських рішень або(та) вчинення дій, вигідних для суб'єкта інформаційного впливу за допомогою використання певним чином організованої інформації та інформаційних технологій.

Суб'єктами проведення СІО можуть бути [5]:

1. Керівництво іноземної держави - головний суб'єкт, всі інші - виконавці.
2. Засоби масової інформації (Іноземні та підконтрольні вітчизняні).
3. Неурядові організації (іноземні й підконтрольні вітчизняні).
4. Спецслужби іноземної держави.
5. Інтернет-ресурси.
6. Агентура впливу іноземних держав та підконтрольні лобістські структури із представників влади, управління, місцевого самоврядування, політичних партій, громадських і релігійних організацій та відомих діячів культури.

СІО можуть бути спрямовані проти населення загалом чи окремих соціальних прошарків і груп; проти політичної, фінансово-економічної, наукової, культурної еліти; проти певних політичних чи військових лідерів; проти релігійних діячів; проти окремих осіб, відповідальних за прийняття тих чи інших суспільнозначимих рішень тощо. Також можуть нести вплив на інформаційно-технічну інфраструктуру, але для більш ефективного впливу- на свідомість і поведінку людей.

СІО становлять складову військових операцій і традиційної війни в цілому, передують їм та супроводжують їх. При цьому *СІО* набувають, як правило, внутрішнього та зовнішнього напрямів, націлені на власну армію і населення, та армію супротивника і його населення, населення сусідніх країн і міжнародну спільноту загалом.

Висновки. Проблема спеціальних інформаційних операцій є об`єктом наукового осмислення протягом не одного століття, проте наукові школи у цій сфері склалися лише у другій половині ХХ ст. Аналіз цієї проблематики ускладнює її закритість.

Створення ефективної системи протидії спеціальним інформаційним операціям для захисту населення від інформаційних впливів і технологій деструктивної зміни свідомості особистості, соціальних груп є досить важливим завданням. Реалізувати це можливо лише комплексно, тобто Україна повинна вжити відповідні правові, організаційні, технічні заходи, аби організувати і забезпечити надійний захист інформаційних джерел від спотворення зацікавлених груп осіб чи країн.

Література:

1. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії :монографія / О. В. Литвиненко. – К. : ВКФ "Сатсанга", 2000.- 89 с.

Клюковський Д.В.
аспірант кафедри вищої математики
Державного університету телекомунікацій, м. Київ, Україна

ТЕХНОЛОГІЇ ТА ОБМЕЖЕННЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

В даній доповіді будуть розглянуті основні технології інтелектуального аналізу даних та обмеження. Основна ідея полягає в тому, що необхідно постійно мати справу з працюючою системою, що накопичує та, в загальному випадку, керує більшістю інформаційних процесів. Результатом розвитку IT, Internet та програмно інформаційних комплексів є дані, які можуть містити доволі цінну інформацію. Знання, як відомо, мають суб'єктивний характер, а їх істинність росте в процесі накопичення досвіду.

Основна суть технологій інтелектуального аналізу даних полягає в пошуку у великих обсягах даних інформації, що може бути неочевидною, об'єктивною або практично корисною. Об'єктивні закономірності повністю відповідають дійсності. Неочевидні - це закономірності, що не виявляються стандартними методами обробки даних чи експертом.

Створення баз даних в різноманітних сферах призвело до накопичення величезних обсягів даних, їх аналізу та обробки. Найбільш поширеними технологіями інтелектуального аналізу даних є Data Mining, Text Mining, Web Mining та OLAP. Різниця між цими технологіями полягає лише в кінцевих методах аналізу та меті що ставиться. Для максимально ефективного використання технологій інтелектуального аналізу даних необхідно виконати наступні кроки: вибрати, очистити, перетворити дані. Результати більшою мірою залежать від рівня підготовки даних для обробки ніж від можливостей алгоритму або множини алгоритмів.

Найбільшою проблемою першого та другого етапу підготовки даних(вибір та очищення) є обмеження надвеликого розміру даних, що аналізуються. Від цього сильно залежить час виконання алгоритмів інтелектуальної обробки даних, що в кінцевому випадку може призвести до втрати актуальності отриманої інформації або не вірній інтерпретації експертом отриманих результатів. Неможливо отримати корисну інформацію без розуміння суті даних, тому на всіх етапах перетворення даних експерт повинен розуміти проблеми, обмеження та поставлені критичні питання.

В доповіді розкриваються цілі вищезазначених технологій, проблем пов'язаних з обмеженнями. Технології інтелектуального аналізу даних не можуть дати відповіді на ті питання, що не були задані. Також не може бути змінений експерт або аналітик, а лише надається потужний інструмент для підвищення можливостей аналізу.

Сталинський Д. А.
студент кафедри Управління інформаційною безпекою
Державний університет телекомунікацій
м. Київ, Україна

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЧНИХ МЕТОДІВ ОРГАНІЗАЦІЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНТЕРНЕТ-БАНКІНГУ

Інформаційна безпека інтернет - банкінгу потребує якісного забезпечення комплексним захистом всіх ланок системи – від захисту серверів та веб-сайту банку до авторизації та шифрування платіжних документів на стороні клієнта.

Для цього використовуються наступні механізми [1]:

- Шифрування даних. Безпека підключення користувачів до інтернет-банкінгу забезпечується використанням протоколів SSL/TLS.
- Багатофакторна авторизація. Застосовується на базі таємних криптографічних ключів, або одноразових паролів (OTP-паролів).
- Електронний цифровий підпис. Механізм електронного цифрового підпису забезпечує автентичність та цілісність електронних платіжних документів.

Крім перерахованого вище, банки найчастіше застосовують додаткові заходи для забезпечення безпечного користування інтернет-банкінгом:

- обмеження використання особистого сертифіката - система деяких банків дозволяє використовувати електронний ключ (електронний сертифікат) тільки на тому комп'ютері, на якому він був згенерований. Таким чином, здійснювати платежі через інтернет-банкінг можна тільки з особистого комп’ютера клієнта.
- віртуальна клавіатура - призначена для того, щоб унеможливити зчитування реєстраційних даних клієнта при введенні їх зі звичайної клавіатури за допомогою кейлогерів ,як програмних так і апаратних.
- обмеження тривалості сесії - у разі неактивності користувача, сесія в системі Інтернет банкінгу через певний час (зазвичай 10-15 хвилин) буде закрита.
- історія підключень - за допомогою цієї функції користувач Інтернет банкінгу дізнається, якщо хтось крім нього підключався до системи, а також зможе відстежити всі несанкціоновані операції, якщо вони були зроблені.

Література:

1. Security Testing Handbook for Banking Applications. Arvind Doraiswamy, Sangita Pakala, Nilesh Kapoor. 2009

Жебка В.В.
доцент кафедри вищої математики
Державний університет телекомунікацій
м. Київ, Україна
Дзядик С.Ю.
доцент кафедри вищої математики
Державний університет телекомунікацій
м. Київ, Україна

ОСНОВНІ АСПЕКТИ ВИКОРИСТАННЯ НЕСКАЛЯРНОЇ ОПТИМІЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ

На сьогодні математичні моделі та методи знайшли широке застосування при проектуванні та управлінні телекомунікаційною мережею з метою отримання оптимального плану рішення.

В деяких технічних завданнях виникають екстремальні задачі, математичний опис яких містить величини, які мають нескалярну природу, тобто визначені не на числовій осі, а на комплексній площині.

Операції, які призводять до задач нескалярної оптимізації:

1. Пошук найкоротшого шляху.
2. Вирівнювання електричного навантаження мережі.
3. Спільне використання активного та реактивного навантаження системи.

Існуючі способи перетворення нескалярних екстремальних задач в скалярні аналоги дають можливість використовувати методи математичного програмування, але при цьому виникає ряд недоліків:

- відхід від природньої нескалярної форми математичного опису;
- втрата аргументу комплексної площини, що є важливою інформаційною характеристикою;
- виникнення неточностей у зв’язку з тим, що додавання і віднімання модулів в загальному випадку є нерівноцінним додаванню і відніманню комплексних величин;
- порушення адекватності математичного опису при виключенні будь-якої складової комплексної величини;
- підвищення в два рази порядку відношень, що представляють модулі;
- збільшення розмірностей математичних моделей.

Нескалярна оптимізація доцільна, оскільки вона зменшує порядок критеріальних функціоналів та обмежень, а також зменшує розмірність моделей порівняно з відповідними математичними моделями, побудованих в термінах скалярної оптимізації.

Жебка В.В.
доцент кафедри вищої математики
Державний університет телекомунікацій
м. Київ, Україна
Гладиш Б.І.
аспірант кафедри геометрії, топології та динамічних систем
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

ОСНОВНІ АСПЕКТИ ТЕОРІЇ КАТАСТРОФ В СИСТЕМІ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНОЮ МЕРЕЖЕЮ

Одним з найважливіших завдань розвитку телекомунікацій є створення ефективної системи управління. Причому, ця система управління повинна працювати як в умовах стаціонарного режиму, так і в надзвичайних ситуаціях. Проте зміни відбуваються постійно. І навіть при плавній зміні умов в системі може виникнути стрибкоподібна зміна. Це можна передбачити за допомогою теорії катастроф.

Математична теорія катастроф направлена на розробку математичних моделей катастроф – найрізноманітніших явищ стрибкоподібної зміни функціонування системи у відповідь на поступову зміну зовнішніх умов, які мають деякі загальні риси.

Об’єктом теорії катастроф є стрибкоподібні переходи системи із одного стану в інший, розриви у поступових, неперервних процесах, раптові якісні зміни поведінки системи.

В будь-якій системі по характерним ознакам можна визначити, що вона містить катастрофу. Ці ознаки мають назву прапори катастроф.

Основні ознаки катастрофи:

1. модальність – це властивість об’єкта системи, яка полягає в тому, що при деяких значеннях управляючих параметрів можливі декілька положень рівноваги системи (декілька мод);
2. недосяжність – в системі одне з положень рівноваги не досягається і не спостерігається;
3. катастрофічні стрибки – стрибкоподібний перехід системи із одного положення рівноваги в інше.
4. гістерезис – перехід системи із одного стану в інший і навпаки при різних значеннях управляючих параметрів;
5. розходження – невелика зміна шляху в просторі параметрів приводить до якісно відмінного кінцевого стану системи.

Зазвичай ці ознаки зустрічаються в сукупності. Вони залежать від досяжності фізичною системою області простору управляючих змінних, в якій потенціал має більш ніж один локальний мінімум.

Як тільки ми знайшли одну з цих ознак, тобто встановили, що відбудеться катастрофа, управляючі параметри можна змінити так, щоб можна було виявити решту ознак, які обов’язково повинні проявити себе при певних умовах.

Існують й інші ознаки катастрофи – розходження лінійного відклику, критичне сповільнення (пом’якшення моди) і аномальна дисперсія. Вони спостерігаються навіть тоді, коли потенціал має лише один локальний мінімум. Ця обставина може бути використана для установлення як критичних значень, так і безпечних меж управляючих параметрів в багатьох випадках, коли неочікувані «катастрофічні стрибки» можуть виявитися пагубними для системи.

Hladysh B.I.
Postgraduate Student of Department of Geometry, Topology and Dynamical Sciences of Mechanics and Mathematics Faculty of Taras Shevchenko National University of Kyiv
State University of Telecommunications
Kyiv, Ukraine

Zhebka V.V.
Associate Professor Department of High Mathematics
State University of Telecommunications
Kyiv, Ukraine

TOPOLOGICAL ASPECTS OF SURFACES BY GENUS 3 WITH BOUNDARY AND OPTIMAL FUNCTIONS DEFINED ON THEM IN TECHNICAL SCIENCES

There are many cases, when functions with the least possible number of isolated critical points on the boundary of the surface is the main object in mathematical model, which is in correspondence to some problems in technical sciences. That is why the issue of examining such type of functions is significant and relevant.

Thus, on compact surfaces with boundary, excepting 2-dimensional disk, optimal functions have three critical points. Let$f$ be a smooth function, defined on the surface$M$with boundary∂M, $p_0 \in \partial M$– isolated critical point of function $f$and its restriction $f|_{\partial M}$ to the boundary. Then this function can be presented in some neighborhood of point p_0 in the next form:

$$f\ x,y\ = Re\ x+iy\ ^n,\quad x,y\ \in\ \ x,y\ \in \mathbb{R}^2\ \ y \geq 0\},n \in \mathbb{N}.$$

Further, we consider the case of previously described neighborhood of isolated critical point (which is not maximum or minimum) on oriented surface by genus 3 with 1 component of the boundary. Such neighborhood can be presented in the form of circle with 14 marked points and 6 chords. These matched points divine the circle into 14 not shadowed and shadowed arcs, which interchange each other. These arcs correspond with sets $V_+ = \ \ x,y\ \in M\ f\ x,y\ > 0$ and$V_- = \ \ x,y\ \in M\ f\ x,y\ < 0$ respectively (here we suppose the equality $f\ p_0\ = 0$).

Previously described circle with arcs calls *arc diagram.* Two arcs diagrams received be symmetry of turn, we call *equivalent*.

Considering such diagrams, we get the number of topological nonequivalent functions of oriented surface by genus 3with 1 component of the boundary, three isolated critical points which belong to the boundary and it is equal to 94.

References:

[1] Полтавець Д.М. Топологія динамічних систем на поверхнях: дис. на здобуття канд.фіз.-мат.наук: 01.01.02. – Диференціальні рівняння / Д. М. Полтавець: – Київ, 1996. – 77с.

к.т.н., доцент КАТКОВ Ю. І., студент КАТКОВ О.Ю
Державний університет телекомунікацій.
Кафедра Комп'ютерних наук та інформаційних технологій
м. Київ, Україна

Аналіз потенційних джерел загроз інформаційній безпеці

Перш ніж приступити до створення системи інформаційної безпеки, необхідно оцінити які загрози є найбільш актуальними. Забезпечення безпеки інформації будь-якої організації (фірми) має ґрунтуватися на глибокому аналізі потенційних загроз. Тому метою даної публікації є розгляд в рамках загальної методології оцінки загроз інформаційній безпеці фірми питань пов'язаних з причинами комп'ютерних злочинів і мотивами тих хто і як їх робить.

Розглянемо загрозу впровадження вірусів так званого "троянського коня" в корпоративне програмне забезпечення зловмисниками, якими можуть бути скривджені працюючі, звільнені співробітники в даній організації або потенційні працівники, яким відмовлено в роботі. Це досить часте явище. Для захисту пропонується використання властивостей віртуальних машин.

Мотивація таких вчинків пов'язана, по-перше, із заниженою оцінкою керівництвом особистих якостей зловмисника, по-друге, із знанням цим зловмисником структури і функцій мережі і порядку використання корпоративної системи електронної пошти. Це створює загрозу за рахунок поширення вірусів типу «троянського коня».

Вихідною умовою для здійснення зловмисником атаки на програмне забезпечення організації є намагання отримати доступ до всіх критичних систем (робочих станцій і серверів, що використовується в організації, наприклад, інформаційних систем відділу кадрів, бухгалтерії та інші). Проблема полягає в тому, що найбільш вразливою ланкою доступу до таких систем є корпоративна система електронної пошти.

Справа в тому, що одним із засобів організації взаємодії між співробітниками будь-якої фірми зазвичай використовується спеціальний поштову адресу на поштовому сервері, який дозволяє тім, хто його знає, відразу посилати повідомлення великій кількості користувачів у цій організації. Технічно це робиться шляхом дозволу користувачам доступу до адресного довідника, яка вбудована в поштову систему, і надання користувачам можливості оновлювати довідник без будь-яких обмежень, а також використанням спеціального ідентифікатора користувача в цьому адресному довіднику як широкомовної адреси. Якщо зловмисник має доступ до адресного довідника з поштового сервера, то він може надіслати листа будь-якому користувачеві, або лист всім користувачам відразу. При цьому йому не потрібно володіти якимись особливими технічними знаннями. Загроза в тому, що може бути відправка по корпоративної пошти зараженого листа з заголовком, який зазвичай використовується керівниками фірми для оповіщення про важливий захід. Як правило до такого листа прикріплюється деякий файл, наприклад, презентація на PowerPoint, яка має формат файлу (* .exe -сам розпаковується), і вказівка, що співробітники повинні розпакувати файл, щоб подивитися презентацію керівника фірми. Насправді ніякої презентації в цьому файлі може і не бути, а файл * .exe, запустить вірус (так званого "троянського коня"). Наприклад, вірус при запуску видаляє весь вміст жорсткого диска на машині користувача. Статистика показує, до 40 % співробітників фірми при отриманні таких листів відкривають такі додатки до листа, не підозрюючи небезпеки.

Рішення проблеми передбачає наступні дії згідно [1-3]:

• Повинен бути встановлений міжмережевий екран і в ньому повинна бути встановлена остання версія програмного забезпечення, що дозволяє сканувати додатки до листів на віруси і відомих троянських коней. Крім того, будь-які додатки, що мають розмір більше певного, віддалялися, а замість них в лист включалося повідомлення про це.

• До користувачів в інструкції політики безпеки фірми повинні бути вказані заходи щодо запобігання подібним загроз, щоб знати, як себе вести в разі повторення подібних ситуацій, наприклад, встановлені спеціальні програми, які дозволяють перегляд вмісту прикріплених файлів без його запуску,

• Треба регулярно перевірятися журнали телефонних дзвінків на специфічні види дзвінків і розмови співробітників зі звільненими співробітниками, яких звільнили не за їх власним бажанням, незабаром після їх звільнення.

• Мати списки машин і рівні доступу співробітників, до яких вони мають доступ, щоб при звільненні системні адміністратори відразу видалили їх акаунти з усіх цих машин.

• На поштовому сервері компанії повинна бути можливість сканування листів на певні слова, щоб своєчасно виявити потенційно небезпечні листи до того, як вони будуть отримані користувачами.

• У всіх критичних системах фірми повинен проводитися регулярно аудит їх використання, і в них повинні були додані програми, які відстежують всі зміни в контрольованих ними базах даних.

• Співробітники повинні створюватися архівних копій критичних даних користувачів на серверах, які регулярно архівуються системними адміністраторами.

Хоча всі ці заходи і не є досконалими, проте вони забезпечують рівень безпеки і є достатніми для протидії відповідним загрозам.

Удосконалення цих заходів може бути здійснено за рахунок створення віртуальних гостевих машин, які мають реальну можливість протидії відповідним загрозам шляхом створення віртуальних почтових скринь на комп'ютерах кожного користувача корпоративної системи електронної пошти. Мова йде про те, що віртуальні машини мають можливість підключення до мережі та установки почтових програм. Таким чином поштові програми на віртуальних гостевих машинах знаходяться як би у "контейнері" без виходу на основну операційну систему.

Практична перевірка такого способу захисту показала досить позитивні результаті за рахунок властивостей віртуалізації процесу обміну повідомленнями.

Джерела:

1. Компьютерные преступления (кто и как их совершает) - http://citforum.ck.ua/security/articles/seccases/seccases.shtml
2. Социальный инжиниринг: Метода атак и способы защиты. - http://bezpeka.ladimir.kiev.ua/pq/show/seminar/html/Web_5.html?news_arch=2015
3. О хакерах. - http://fdjyakov.zz.vc/story2.htm

В.В. Бугаенко, с.н.с.
ДП «Український науково-дослідний інститут зв'язку»

СТУПЕНЧАТАЯ АППРОКСИМАЦИЯ СИНУСОИДЫ С МИНИМАЛЬНЫМ КОЛИЧЕСТВОМ СТУПЕНЕК

При формировании синусоидальных сигналов цифровыми генераторами с использованием ступенчатой аппроксимации для уменьшения погрешности аппроксимации требуется увеличение количества ступенек, что несложно для низких и ультранизких частот [1]. Однако практически могут возникнуть причины, препятствующие этому увеличению, например, недостаточное быстродействие цифро-аналоговых преобразователей (ЦАП) при формировании синусоиды более высокой частоты.

Предлагается аппроксимация полуволны синусоидального сигнала симметричной ступенчатой трапецией соответствующей полярности с числом степенек п = 6 (рис.1)

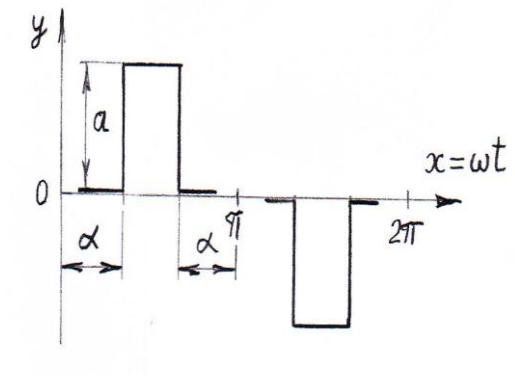

Рис. 1

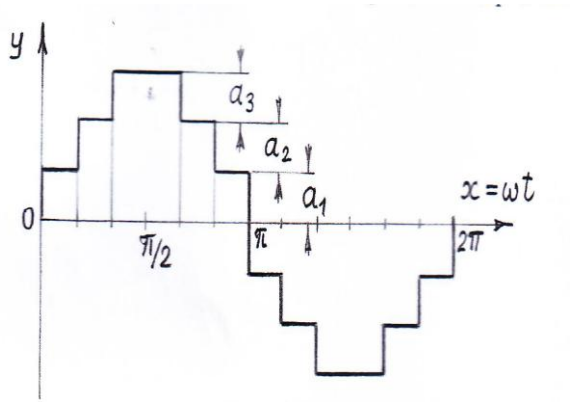

Рис. 2

Трапеция образуется суммированием трех импульсных сигналов, показанных на рис. 2, формула разложения в ряд Фурье которых имеет вид [2] :

$$y = \frac{4a}{\pi}\ \cos\mathcal{L}\sin x + \frac{1}{3}\cos 3\,\mathcal{L}\sin 3x + \frac{1}{5}\cos 5\,\mathcal{L}\sin 5x + \cdots$$

Разложение первого сигнала при $\mathcal{L}_1 = 0$:

$$y_1 = \frac{4a_1}{\pi}(\sin x + \frac{1}{3}\sin x\ + \frac{1}{5}\sin 5x + \frac{1}{9}\sin 9x + \frac{1}{11}\sin 11x +$$

$$+\frac{1}{13}\sin 13x + \frac{1}{15}\sin 15x + \frac{1}{17}\sin 17x + \cdots)$$

Для второго сигнала при $\mathcal{L}_1 = \frac{\pi}{6}$:

$$y_2 = \frac{4a_2}{\pi}(\frac{\overline{3}}{2}\sin x - \frac{1}{5}\frac{\overline{3}}{2}\sin 5x\ - \frac{1}{7}\frac{\overline{3}}{2}\sin 7x + \frac{1}{11}\frac{\overline{3}}{2}\sin 11x +$$

$$+\frac{1}{13}\frac{\overline{3}}{2}\sin 13\,x-\frac{1}{15}\frac{\overline{3}}{2}\sin 15\,x+\frac{1}{17}\frac{\overline{3}}{2}\sin 17\,x+\cdots)$$

Для третьего сигнала при $\mathcal{L}_3=\frac{\pi}{3}$:

$$y_3=\frac{4a_3}{\pi}(\frac{1}{2}\sin x-\frac{1}{3}\sin 3\,x\ +\frac{1}{5}\cdot\frac{1}{2}\sin 5\,x+\frac{1}{7}\cdot\frac{1}{2}\sin 7\,x-\frac{1}{9}\sin 9\,x+$$

$$+\frac{1}{11}\cdot\frac{1}{2}\sin 11\,x+\frac{1}{13}\cdot\frac{1}{2}\sin 13\,x-\frac{1}{15}\sin 15\,x+\frac{1}{17}\cdot\frac{1}{2}\sin 17\,x+\cdots)$$

Суммирование сигналов y_1 и y_3 при $a_1=a_3=a$ взаимно компенсирует нечетные гармоники, кратные трем:

$$y_1+y_3=\frac{4a}{\pi}(\frac{3}{2}\sin x+\frac{1}{5}\cdot\frac{3}{2}\sin 5\,x\ +\frac{1}{7}\cdot\frac{3}{2}\sin 7\,x+\frac{1}{11}\cdot\frac{3}{2}\sin 11\,x+$$

$$+\frac{1}{13}\cdot\frac{3}{2}\sin 13\,x+\frac{1}{17}\cdot\frac{3}{2}\sin 17\,x+\frac{1}{19}\cdot\frac{3}{2}\sin 19\,x+\cdots)$$

Если $a_2=a\ \ \overline{3}$, то в сумме трех сигналов исчезают 5-я и 7-я гармоники:

$$y_1+y_2+y_3=\frac{4a}{\pi}\ \ 3\sin x+\frac{1}{11}3\sin 11\,x\ +\frac{1}{13}3\sin 13\,x+\frac{1}{17}3\sin 17\,x+\cdots\ \ =$$

$$=\frac{12a}{\pi}(\sin x+\frac{1}{11}\sin 11\,x+\frac{1}{13}\ \sin 13x+\frac{1}{17}\sin 17\,x+\frac{1}{19}\sin 19\,x\ldots)$$

Таким образом, в результирующем сигнале отсутствуют все четные гармоники и нечетные гармоники, кратные трем, причем ближайшей является 11-я гармоника, которую легко отфильтровать. Коэффициенты гармоник и нелинейных искажений описанного сигнала равны соответственно 15 и 14,8 %.

Эта аппроксимация синусоиды была использована в разработанном в УНДІЗ датчике скачков уровня и скачков фазы согласно Рек. 0.95 МККТТ для получения контрольного сигнала частотой 1020 Гц.

Литература:

1. Мирский Г.Я. Электронные измерения.−М.: Радио и связь, 1986, с.380.
2. Бронштейн И.Н. и Семендяев К.А. Справочник по математике.−М.: Гос. изд-во технико-теоретической литературы, 1956, с. 555.

І. С. Виноградов
Державний університет телекомуникацій ,
м.Київ, Україна

Методы защиты компьютерной сети организации от НСД из сети Интернет. Применение межсетевых экранов

В сучасному світі величезна кількість мереж об'єднана за допомогою Інтернет. Тому очевидно, що для безпечної роботи такої величезної системи необхідно вживати певних заходів безпеки, оскільки практично з будь-якого комп'ютера можна отримати доступ до будь-якої мережі будь-якої організації, причому небезпека значно зростає з тієї причини, що для взлому комп'ютера до нього зовсім не потрібно фізичного доступу.

Згідно з даними, отриманими Інститутом комп'ютерної безпеки (Computer Security Institute) в результаті нещодавно проведеного дослідження, у 70% організацій були зламані системи мережевого захисту, крім того, 60% виявлених спроб зломів виходили з внутрішніх мереж організацій.

З огляду на ці факти, можна з упевненістю сказати, що проблема безпеки мереж залишається невирішеною і на сьогоднішній день, оскільки у переважної більшості компаній не вирішені питання забезпечення безпеки, в результаті чого вони несуть фінансові збитки.

Згідно з актуальністю захисту комп'ютерної мережі організації від НСД з мережі Інтернет завдання дослідження є: оцінити можлівість застосування міжмережевих екранів; розглянути основні типи міжмережевих екранів.

Одним з рішень проблем безпеки підключення до мережі Інтернет є застосування міжмережевих екранів. Брандмауер - це програмно-апаратна система, що знаходиться в точці з'єднання внутрішньої мережі організації і Інтернету і здійснює контроль передачі даних між мережами.

Основні типи міжмережевих екранів:

- Мостикові міжмережеві екрани
- Мережеві екрани з фильтрацією пакетів
- Шлюз сеансового рівня
- Шлюз прикладного рівня

Ознайомившись з описаними проблемами, можна зробити висновок, що міжмережеві екрани забезпечують захист комп'ютерної мережі організації від несанкціонованого втручання. Міжмережеві екрани є необхідним засобом забезпечення інформаційної безпеки. Вони забезпечують першу лінію оборони. При виборі і придбанні міжмережевих екранів необхідно ретельно все продумати і проаналізувати. Вибрати потрібну архітектуру і компоненти брандмауера. Правильно налаштувати програмне забезпечення і тестувати конфігурацію брандмауера.

Жданова Ю.Д.,
Доцент каф. Інформаційної та кібернетичної безпеки
Шевченко С.М.
Доцент каф. Вищої математики
Державний університет телекомунікацій
м. Київ, Україна

КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ

Користувачі, які бажають обмінятися захищеною інформацією, повинні мати спільний секретний ключ. Задача конфіденційної доставки ключової інформації вирішується методами асиметричної криптографії. Проте досі не існує математичних доказів однонапрямленості функцій, використовуваних в асиметричних криптоалгоритмах. Зростання продуктивності комп'ютерів змушує збільшувати розмір використовуваних ключів і складність односторонніх функцій. Нові технології – квантова механіка – переводять експоненціальні задачі в розряд задач, розв'язуваних за поліномиальний час.

Квантова криптографія в принципі дозволяє реалізувати абсолютно стійкі системи шифрування з одноразовими ключами Секретність ключів у квантовій криптографії заснована на фундаментальних заборонах квантової механіки, а саме, на тій обставині, що пара спостережуваних, яким відповідають некомутуючі оператори, не може бути достовірно одночасно помітна, що є наслідком співвідношення невизначеності Гейзенберга. В квантовій криптографії в якості таких спостережуваних виступають матриці щільності інформаційних станів, відповідних класичним бітам 0 і 1.

В квантовій криптографії крім квантового каналу зв'язку (в реальних умовах це або оптоволокно, або відкритий простір), по якому передаються квантові стани, необхідний також класичний відкритий канал зв'язку, за допомогою якого легітимні користувачі з'ясовують зміни статистики відліків і корекції помилок в первинному ключі, переданому по квантовому каналу.

Щоб виключити можливість створення перешкод для встановлення зв'язку між легітимними користувачами по квантовому каналу, були запропоновані протоколи передачі ключової інформації BB84 і B92. Найважливішою характеристикою протоколів квантової криптографії є допустима критична помилка на приймальній стороні, до якої можливо секретне розповсюдження ключів.

Криптостійкість протоколу B92 базується на тому, що при спробі виміряти криптоаналитиком стан фотона, вноситься помилка в інший неортогональний стан даних. Таким чином, легітимні користувачі спільними зусиллями можуть виявити існування перехоплювача.

Литература:

1. Bennett C. H., Brassard G., «Quantum Cryptography: Public Key Distribution and Coin Tossing», Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.
2. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. –М.: Мир, 2006.– 824 с.

Крушець А.О.
Державний Університет Телекомунікацій
м. Київ, Україна

ОСНОВНІ МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Необхідно пам'ятати, що інформація в системах електронних платежів – це реальні гроші, фінансова, персональна або інша конфіденційна інформація. Загрозою для якої є несанкціонований в тому числі випадковий, доступ до неї, результатом якого може стати знищення, зміна, блокування, копіювання, а також поширення даної інформації.

Одним з найбільш вразливих місць в системі електронних платежів є пересилання платіжних (перекази) та інших повідомлень між банками, між банком і банкоматом, між банком і клієнтом.

При цьому виникають наступні типи проблем:

1. Захист документів, які передаються каналами зв'язку (забезпечення їхньої цілісності та конфіденційності);
2. Захист самого процесу обміну документами (проблема доведення факту відправки (отримання) документа).

Саме тому у системах електронних платежів мають бути реалізовані механізми, що забезпечують реалізацію функцій захисту та політики безпеки на окремих вузлах СЕП, та на рівні протоколів високого рівня:

1. Механізми шифрування, які забезпечують конфіденційність даних, що передаються.
2. Механізми цифрового підпису, які містять процедури закриття блоків даних та перевірки закритого блоку даних.
3. Механізми контролю доступу.
4. Механізми забезпечення цілісності даних, що передаються.
5. Механізми автентифікації об'єктів (абонентів) платіжної системи.
6. Механізми заповнення тексту використовують для забезпечення захисту від аналізу трафіка.
7. Механізми управління маршрутизацією забезпечують вибір маршрутів руху інформації по комунікаційній мережі таким чином, щоб виключити передачу секретних даних по небезпечним та ненадійним каналам.
8. Механізми засвідчення (арбітр).
9. Виявлення і обробка подій (аналогічно до засобів контролю небезпечних подій).
10. Звіт щодо перевірки небезпеки (аналогічно до перевірки з використанням системного журналу) на відповідність цій ПБ.

Таким чином, саме використання різних криптографічних алгоритмів на різних етапах обробки електронних банківських документів дає змогу забезпечити безперервний захист інформації в інформаційній мережі, а також відокремлену обробку інформації стосовно різних задач інформатизації Національного банку.

Литература:

Задірака В.К., Олексюк О.С. Методи захисту банківської інформації. (1999 г.)

Кононський О.Д.
Державний університет телекомунікацій
м. Київ, Україна

КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Система електронного документообігу є технологічною основою діяльності державних та приватних підприємств по обробці, прийняттю та виконанню рішень. Зі збільшенням кількості конфіденційних документів в органах державної влади і організаціях різної форми власності, активним переходом систем документообігу до електронного вигляду, збільшується потреба в системах захищеного електронного документообігу.

Необхідно чітко оцінювати можливі загрози і ризики та можливі втрати від реалізованих загроз.

Основні загрози для систем електронного документообігу:

1. загроза цілісності – пошкодження, знищення або спотворення інформації, що може бути як ненавмисним у випадках помилок і збоїв, так і навмисним;
2. загроза конфіденційності – будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації, зміна маршрутів слідування і т.д.;
3. загроза працездатності системи – загроза, реалізація якої призводить до порушення або припинення роботи системи, включаючи навмисні атаки, помилки користувачів, а також збої в обладнанні та програмному забезпеченні;
4. неможливість доказу авторства – якщо не використовується електронний цифровий підпис, то неможливо довести, що саме даний користувач створив даний документ;
5. загроза доступності – загроза, що порушує можливість за допустимий час отримати потрібну інформацію користувачам, що мають право доступу до неї.

Захист саме від цих загроз в тій чи іншій мірі повинна реалізовувати будь-яка система електронного документообігу.

Відповідно, в комплекс захисту електронних документів повинні входити наступні заходи:

1. обмеження прав фізичного доступу до об’єктів системи документообігу;
2. розмежування прав доступу до файлів і папок;
3. підтвердження авторства електронного документу;
4. контроль цілісності електронного документу;
5. конфіденційність електронного документу;
6. забезпечення юридичної сили електронного документу;
7. забезпечення надійності функціонування технічних засобів;
8. забезпечення резервування каналів зв’язку;
9. резервне дублювання інформації;
10. захист від вірусів;
11. захист від "зламу" мереж.

Підхід до захисту електронного документообігу повинен бути комплексним. Необхідно оцінювати можливі загрози і ризики, величину можливих втрат від реалізованих загроз. Захист електронного документообігу не зводиться лише до захисту документів і розмежування доступу до них. Залишаються питання захисту апаратних засобів системи, персональних комп'ютерів, принтерів, захисту мережі, в якій функціонує система, захисту каналів передачі даних і мережевого обладнання.

Литература:

1. Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота // Компьютерное обеспечение и вычислительная техника. – 2009. – № 6. – С. 140–143.
2. Сабанов А.А. Некоторые аспекты защиты электронного документооборота //Connect! Мир связи. – 2010. – № 7. – С. 62–64.
3. Джхунян, В.Л. Электронная идентификация / В.Л. Джхунян, В.Ф. Шаньгин. – М.: NT Press, 2009. – 695 с.

Савченко Д. С.
аспірант кафедри інформаційних систем і технологій та захисту інтересів держави у сфері інформаційної безпеки
Національна академія Служби безпеки України
м. Київ, Україна
Удуд Н. О.
студент 4-го курсу Навчально-наукового інституту інформаційної безпеки
Національна академія Служби безпеки України
м. Київ, Україна

АВТОМАТИЗАЦІЯ ПОШУКУ І ВИПРАВЛЕННЯ ПОМИЛОК ПРИ ОБРОБЦІ НЕСТРУКТУРОВАНИХ ТЕКСТІВ

Особливістю неструктурованих текстів – тобто текстів, викладених природною мовою людини, є наявність у них випадкових помилок, в першу чергу тих, що пов'язані із неправильним написанням окремих слів. Внаслідок цієї обставини сучасні системи з автоматизованої обробки таких текстів повинні бути здатними виявляти та виправляти подібні помилки.

Задача виявлення та виправлення зазначених помилок традиційно вирішується через оцінювання схожості (або розбіжності) між кожним словом тексту, та записами у словнику автоматизованої системи. При цьому в першу чергу інтерес становлять такі методи оцінювання схожості слів, що були б максимально наближеними до рішень, одержаних за допомогою експертів.

Для кількісної оцінки схожості слів з дотриманням зазначеного принципу можна використовувати метод аналізу співпадіння символів і біграм (комбінацій з 2-х сусідніх символів), з яких вони складаються, на основі коефіцієнту схожості Серенсена.

Сутність такого методу полягає у наступному.

Розглянемо слова X та Y довжиною відповідно n та m символів. Вважатимемо умовно, що перед і після кожного із цих слів знаходяться пусті символи. Розкладемо слова X та Y на біграми, починаючи з їх перших пустих символів і закінчуючи їх останніми пустими символами. Тоді слово X утворить $n+1$ таких біграм, а слово Y утворить $m+1$ біграм. Розкладемо додатково слова X та Y на окремі символи. Позначимо всі символи і біграми в слові X, які присутні також у слові Y. Підрахуємо вагу позначених символів і біграм: кожний символ та біграму з пустим символом зарахуємо як 2 умовні одиниці ваги, а кожну біграму із двох символів – як 1 одиницю ваги.

Тоді кількісну оцінку схожості σ_{XY} слів X та Y можна визначити за наступною формулою на основі коефіцієнту схожості Серенсена:

$$\sigma_{XY} = \frac{2W}{3(n+m+2)}, \qquad (1)$$

де: n – кількість символів у слові X, m – кількість символів у слові Y, W – сума ваги символів і біграм, однакових для обох слів.

Як видно з формули (1), кількісна оцінка схожості двох однакових слів завжди дорівнює 1, а кількісна оцінка схожості слів, у яких немає жодного спільного символу, завжди дорівнює 0. В інших випадках кількісна оцінка схожості, як і потрібно, знаходиться в діапазоні $(0;1)$.

Наприклад, розглянемо схожість слів „ТЕКСТ" і „ТЕСТ". Перше слово утворює наступну сукупність символів і біграм: „Т", „Е", „К", „С", „Т", „¤Т", „ТЕ", „ЕК", „КС", „СТ", „Т¤". Друге слово утворює наступну сукупність символів і біграм: „Т", „Е", „С", „Т", „¤Т", „ТЕ", „ЕС", „СТ", „Т¤". Як видно, 8 з них спільні: "Т", "Е", "С", "Т", „¤Т", "ТЕ", "СТ", „Т¤". Їх вага дорівнює 14 одиниць, а кількісна оцінка схожості слів становить 28/33 або приблизно 0,85.

Отже, запропонована інтерпретація схожості слів враховує не тільки кількісне співпадіння їх символів, але й також співпадіння порядку слідування цих символів, при цьому враховуються не абсолютні, а саме відносні позиції символів.

Важливим недоліком для практичного використання зазначеної оцінки схожості слів в контексті вирішення завдань з автоматизованої обробки неструктурованих текстів є неможливість уникнути повного перебору словника і подальшого сортування результатів для встановлення кожного разу найбільш імовірних еквівалентів словникових статей для заданого текстового фрагменту.

Література:

1. Левенштейн В. И. Двоичные коды с исправлением выпадений, вставок и замещений символов / Докл. Академий Наук СССР, 1965. С. 845-848. [т.163.4]

2. Hyyrö H., Navarro G. Faster bit-parallel approximate string matching. In Proc. 13th Combinatorial Pattern Matching (CPM'2002), LNCS 2373, pages 203-224, 2002.

3. Navarro G. A guided tour to approximate string matching. ACM Computing Surveys, 33(1):31-88, 2001.

4. Sörensen T. A method of establishing groups of equal amplitude in plant sociology based on similarity of species content // Kongelige Danske Videnskabernes Selskab. Biol. krifter. Bd V. № 4. 1948. P. 1-34.

Лісковський І.О.
Зав. кафедри, кандидат технічних наук, професор кафедри фізики Державного університету телекомунікацій
Морозова С.В.
ст. викладач кафедри фізики Державного університету телекомунікацій

ОГЛЯД МЕТОДІВ КОНТРОЛЮ ЯКОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

Тези

Мобільний телефонний зв'язок сьогодні — це одна з найбільш успішних та дуже динамічних за розвитком областей радіозв'язку. Все більша кількість людей користується мобільними телефонами як звичайним та необхідним засобом комунікації.

Сьогодні в Україні налічується вже більш ніж 62 млн абонентів різних мобільних операторів. Рівень проникнення мобільного зв'язку складає близько 130%. За 10 років, починаючи з 2003 року, кількість абонентів мобільного зв'язку збільшилася майже в 10 разів (6,5 млн. абонентів в 2003 році і 62 млн. за станом на кінець 2013 року). Так само, як і кількість абонентів, стрімко змінюється і саме поняття мобільного телефону і мобільного зв'язку. Нам вже недостатньо просто телефонних дзвінків чи смс, мобільний телефон став основним засобом комунікації, невід'ємною складовою нашого життя. З'явилося поняття «мультисервісна мережа», спектр послуг, що надаються, розширюється з кожним днем. Користувачі розширюють свої вимоги до кількості та якості сервісів. Тому перед операторами мобільного зв'язку в умовах високої конкуренції та користувацької освіченості стоїть завдання забезпечення заявленого рівня якості обслуговування.

Виходячи з цих умов, постає питання контролю за якістю послуг, що надаються оператором мобільного зв'язку. Таким чином, управління якістю послуг, що надаються забезпечить оператору телекомунікацій підтримувати систему з гарантованим рівнем якості.

Складність побудови системи управління якістю заключається в таких основних факторах :

1) Багато абонентів;
2) Багато параметрів, які потребують контролю за якістю;
3) Велика кількість сервісів, для яких потрібно розробити систему управління;
4) Розміщення обладнання для збору інформації;
5) План здійснення збору інформації;
6) Вибір типу перевірки: суцільна чи вибіркова.

Отже, створення системи управління якістю послуг, що надаються являється актуальною задачею, що стоїть перед операторами телекомунікацій при розвитку мережі в сторону мультисервісності цієї мережі. При створенні даної системи необхідно визначитися з методами, завдяки яким можливо проводити оцінку та вимірювання якості надання телекомунікаційних послуг.

2.1 Основи статистичного забезпечення якості

Статистичне забезпечення якості (СЗЯ) є областю статистики, що займається застосуванням статистичних методів в забезпеченні якості, а особливо застосування статистичних методів в галузі контролю якості.

Види контролю

Забезпечення і підвищення якості продукції, що випускається - одне з головних завдань виробництва. У вирішенні цього завдання важлива роль відводиться контролю якості на всіх етапах виробництва з метою перевірки відповідності показників якості встановленим вимогам. Різноманіття видів контролю якості викликає необхідність їх

систематизації та класифікації за рядом ознак. Класифікація видів контролю якості продукції представлена на рисунку 2.1.

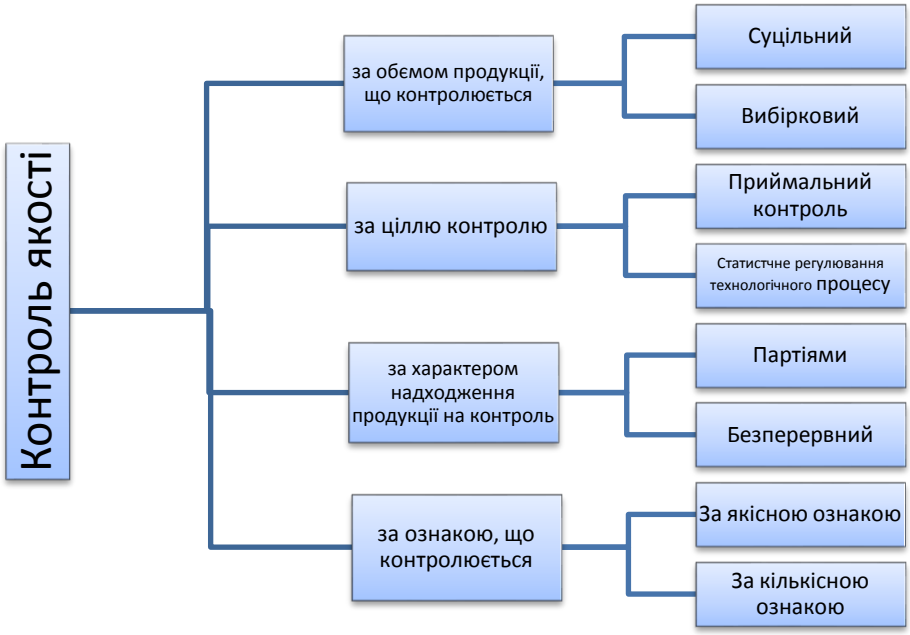

Рисунок 2.1 Види контролю якості продукції

Залежно від складності об'єкта контролю розрізняють централізований контроль технічних або природних об'єктів і складних технологічних процесів і допускового контроль виробів.

За ступенем повноти охоплення контролем вироблених виробів розглядаються два типи контролю .

1 . Суцільний контроль , при якому процедурі контролю піддаються всі вироблені вироби .

2 . Вибірковий або статистичний контроль , при якому процедурі контролю підлягають тільки деякі частки (вибірки) вироблених виробів.

Задачею статистичного забезпечення якості є контроль відповідності між заданими величинами якості послуги з допустимими діапазонами їх змін та самою послугою.

Статистичне забезпечення якості передбачає не суцільний, а вибірковий контроль. Інколи, можливо, що з деяких причин вибірковий контроль недостатній, тоді проводять суцільний контроль.

За місцем , займаному в процесі виробництва виробів , допусковий контроль поділяється на три види .

1 . Вхідний контроль - це контроль матеріалів , заготовок і напівфабрикатів , придбаних на стороні і необхідних для реалізації виробничого процесу .

2 . Технологічний контроль - це сукупність операцій контролю , супроводжуючих все стадії реалізації виробничого контролю .

3 . Вихідний контроль - це контроль готової продукції .

Висновки. Виходячи зі специфіки галузі телекомунікації, доцільно обрати вибірковий метод контролю якості, що дозволить використовувати ресурси компанії для досягнення мети контролю.

Buryachok V., Gulak G., Sokolov V.
State University of Telecommunications

CONSTRUCTION OF THE SPECTRUM ANALYZERS NETWORK 2.4–2.5 GHZ BAND

Network spectrum analyzers may be used for real-time monitoring of network status, and the occurrence of unauthorized devices from their positioning. All these measures are designed to increase the level of security of the wireless network.

We implemented a lot of spectrum analyzers for the 2.4–2.5 GHz ISM band to connect via USB-interface. For example, Ubiquiti AirView2, MetaGeek Wi-Spy, Wi-Detector, as well as on the basis of different sets of debugging (such as TI eZ430-RF2500) or network interface cards (eg, Atheros AR92xx and AR93xx with spectral scan mode).

These devices have a number of drawbacks: the price; the difficulty of obtaining data that are usually tied to a particular program; the inability to change the firmware of devices. In addition, there are of course many projects, homemade, usually based on TI CC2500 chip and Cypress 693x, as well as modules on their basis. But these devices are not suitable for mass production. To build a network spectrum analyzer modules Pololu Wixel good fit.

Module Pololu Wixel (see. Fig. 1) makes it possible to solve this problem. It is built on the chip TI CC2511F32, which is a microcontroller with built-in radio module TI CC2500. Due to the implementation of the 256 available only in advance of reserved channels on which you can record the signal levels [1]. The device is designed primarily for the American market, because not cover the entire frequency range from 2403.5 to 2476.5 MHz. As a result, the frequency channel spacing is 286.4 kHz, which is ahead of many commercial samples. In addition, possible to add external controls directly to the device itself.

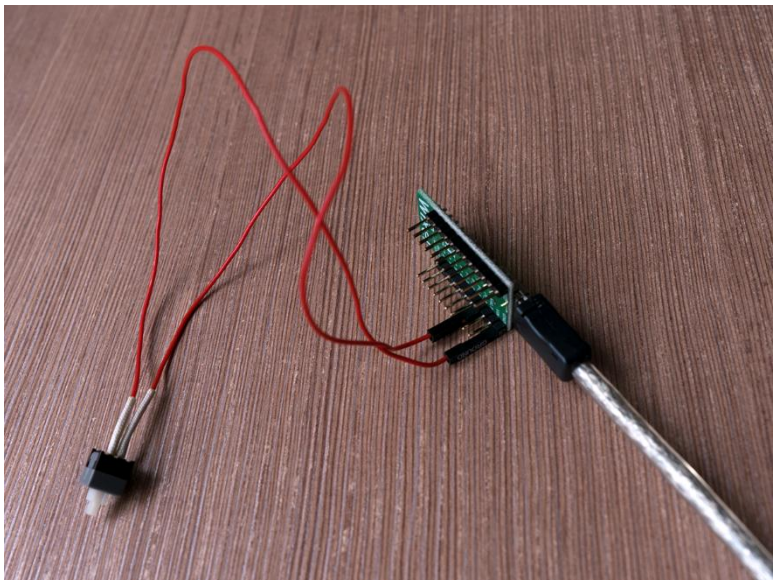

Fig. 1. General view of the device with a button

This device needs to collect the number of samples per channel (approximately a hundred), then use the fast Fourier transform calculates the signal level and the value of averages. On reading one channel it takes an average of 1.6 ms at full bore of about 414 ms channels.

To obtain data on different operating systems, you can use scripts with automatic detection of the connected COM-devices.

Literature

1. Remington, S. James. Spectrum analyzer app code. Source: https://forum.pololu.com/t/spectrum-analyzer-app-code/3394

Складанний П.М.
аспірант кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій

ВИБІР ОПТИМАЛЬНОГО ПІДХОДУ ДО ВИЯВЛЕННЯ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ЗОБРАЖЕННІ

Комп'ютерні мережі, в сучасних умовах, стали одним з вагомих інструментів для передавання величезних потоків мультимедійних повідомлень, які в свою чергу можуть бути використані для приховування інформації. Зважаючи на можливість використання стеганографічних методів для реалізації неправомірних заходів, **актуальною темою** є питання використання стеганоаналізу. Стеганоаналіз – наука про вивчення методів виявлення існування секретної інформації у відкритих повідомлення. У сучасному стеганоаналіз виокремлюють два підходи дій зловмисника:

активний – намагання знищити приховувану інформацію у відкритому повідомленні;

пасивний – полягає у виявленні фактів існування, а також знаходження секретної інформації.

Метод заміни найменш значущого біта на сьогодні є найпоширенішим методом стеганографічного приховування даних. Метод полягає у заміні від одного до чотирьох молодших бітів у байтах кольорового подання пікселів вихідного зображення бітами повідомлення, яке приховується. Даний метод застосовується для растрових зображень, які представляються у форматі без компресії. Одним з таких форматів є BMP. Перевагами цього формату є:

висока якість зображення;

простота формату.

Ці критерії роблять формат BMP найбільш популярним для застосовування його, як контейнера.

Наступний **метод стеганографічного перетворення інформації**, полягає у використанні особливостей файлів, тобто стисненню із втратою даних. Найпоширенішим графічним форматом, який використовую алгоритми стискання даних з втратами, є графічних формат JPEG. В JPEG-файлі інформація приховується не колірних складових окремих пікселів, а приховування відбувається в бітах квантованих дискретних косинусних коефіцієнтів. Файли цього формату дозволяються, з точки зору стеганографії, приховувати досить великі обсяги інформації [1,2,3].

Зважаючи на усе вище зазначене постає **проблема** вибору оптимального підходу до виявлення стеганографічного приховування інформації у зображенні. У роботі досліджено та розглянуто основні методи аналізу, які використовуються для виявлення факту прихованої передачі інформації у графічних файлах.