ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.56.5(043.2)

Борозніченко В.О.
Національний авіаційний університет, Київ

АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

На сьогоднішній день інформаційна сфера є ведучою в діяльності держави і чинить вплив на всі елементи соціальних комунікацій. Динамічний розвиток інформаційної сфери спричиняє виникнення інформаційних ризиків і вразливостей захисту інформації. Всі суб′єкти інформаційних взаємин - держава, суспільство, юридичні та фізичні особи – є власниками інформаційних ресурсів, які потребують певного рівня захисту.

Одним і з першочергових етапів побудови комплексних систем захисту інформації є оцінка інформаційних ризиків. З цією метою в інформаційних системах використовуються спеціальні програмні засоби оцінки інформаційних ризиків.

З огляду на це мета наукового дослідження полягає в наступному: проведення аналізу програмних засобів управління інформаційними ризиками; розробка класифікації програмного забезпечення управління інформаційними ризиками, з умов вимог та можливостей суб'єкта інформаційних відносин.

Наукова новизна дослідження полягає в наступному: розроблено класифікацію програмного забезпечення управління інформаційними ризиками, з урахуванням базових можливостей актуальних програмних продуктів згідно сучасних стандартів інформаційної безпеки.

Проведено оцінку можливостей, якості та ефективності використання програмних засобів оцінки інформаційних ризиків. COBRA- засіб для на аналізу та управління інформаційними ризиками, згідно вимог ISO 17799 у вигляді тематичних запитів. RA Software Tool- засіб, який виконує оцінку інформаційних ризиків згідно вимог стандартів ISO 17799 та ISO 13335. CRAMM- програмний засіб, який доцільно використовувати для аналізу інформаційних систем з підвищенними вимогами до інформаційної безпеки, велика точність пошуку ризиків, можливість заощадження матеріальних ресурсів. RiskWatch- потужний засіб для проведення аудиту інформаційної безпеки, в якості критеріїв для оцінки та управління ризиками використовують представлення річних затрат. OCTAVE використовується для оцінки ризиків за допомогою послідовності організованих внутрішніх семінарів, розташованих відповідним чином. Digilal Security Office- засіб для розробки та управління політики безпеки інформаційної системи на основі стандартів ISO 17799, ISO 27001, ISO 27005. RA2 art of risk- для проектування та побудови системи управління інформаційної безпеки використовується процесний підхід, на базі ISO 17799.

Науковий керівник – О.К..Юдін, д.т.н., проф.

УДК 004.056.5 (043.2)

Волохович Л.С.
Національний авіаційний університет, Київ

МЕТОДИ ОЦІНКИ РИЗИКІВ

На сьогоднішній день актуальним є питанням розробки системи оцінки ризиків, яка за короткий час ґрунтовно буде описувати інформаційну систему, її ресурси, загрози та вразливі місця. Результати оцінки ризику допоможуть спрямовувати та визначити відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки.

В даній роботі проаналізовано системи оцінки ризиків, які можна б було використовувати для адекватної оцінки ризиків та для впровадження до інформаційних систем за короткий час. Так, постає необхідність в досліджені існуючих систем оцінки ризиків та розробки алгоритму проведення аналізу захищеності інформаційних ресурсів.

При впровадженні різних засобів захисту необхідно визначити баланс між можливим збитком від несанкціонованого витоку інформації та розміром вкладень, які витрачені для забезпечення захищеності інформаційних ресурсів.

Ціль оцінки ризику полягає в тому, щоб визначити ризик витоку інформації з корпоративної мережі підприємства. Такі програмні продукти, як: Risk Watch, CRAMM, COBRA, Авангард, ГРИФ,Конкор+ базуються на різних підходах до аналізу ризиків і рішенню різних завдань.

Програмне забезпечення RiskWatch є засобом для аналізу та управління ризиками, більше орієнтоване на точну кількісну оцінку співвідношення втрат від загроз безпеки та витрат на створення системи захисту.

Обстежити інформаційну систему, провести аудит відповідно до вимог стандарту BS 7799, розробити політику безпеки, можна за допомогою метода CRAMM. Даний комплекс робить оцінку ризиків за різними інформаційнми ресурсами, підраховує сумарний ризик ресурсів, а також веде підрахунок співвідношення збитку й ризику й видає недоліки існуючої політики безпеки.

Розглянуті методики дозволяють оцінити рівень поточного стану інформаційної безпеки автоматизованої системи, знизити потенційні втрати шляхом підвищення стійкості функціонування корпоративної мережі, розробити концепцію й політику безпеки автоматизованої системи, а також запропонувати плани захисту від виявлених загроз та вразливих місць. На сьогоднішній день існують різноманітні й складні по своїй структурі автоматизовані системи, для яких неможливо підібрати конкретну методику оцінки ризиків, тому для одержання адекватних результатів оцінки необхідно використати комплексний підхід до оцінок ризиків на основі вже існуючих методик.

Науковий керівник - А.Б.Петренко, к.т.н.,доц.

УДК 004.056.52.57.087 (043.2)

Галата Л.П.
Національний авіаційний університет, Київ

БЕЗПЕКА WINDOWS SERVER 2012. ДИНАМІЧНИЙ КОНТРОЛЬ ДОСТУПУ

Сучасні організації все більшою мірою потребують таких компонентів, як гнучкість і здатність швидко реагувати на нові можливості і технології, і одночасно персонал потребує доступу до даних і інформації незалежно від інфраструктури, мережі, пристроїв, або додатків для їх отримання. Виконання вимог нормативних документів по інформаційній безпеці і потреба в захисті конфіденційної інформації – одні з найважливіших проблем для бізнесу і IT.

Наявні в Windows Server 2012 рішення, які використовуються для ідентифікації і забезпечення безпеки, дають IT-фахівцям можливість гнучкої підтримки нового сучасного стилю роботи і технологій хмарних обчислень.

Завдяки появі функції динамічного контролю доступу (Dynamic Access Control, DAC), ОС Windows Server 2012 кардинально змінила підхід до управління ідентифікацією і доступом до даних.

Dynamic Access Control — перший приклад використання заявок (claim) в базовій моделі авторизації Windows. Такого роду доступ забезпечує недоступний у минулому рівень деталізації і гнучкості.

Windows Server 2012 забезпечує нові, розширені способи управління доступом до Ваших файлів, надаючи зареєстрованим користувачам ресурси, яких вони потребують, за допомогою наступних можливостей:

- класифікація: ідентифікація даних за допомогою автоматизованої і ручної класифікації файлів (File Classification Infrastructure, FCI). Наприклад, можна забезпечити тегами дані на файлових серверах по всій організації;
- контроль: управління доступом до класифікованих файлів по всіх серверах, застосовуючи гарантію (safety net) з використанням централізованих політик доступу (Central Access Policies, CAPs);
- аудит: проводити аудит доступу до файлів на файлових серверах, використовуючи централізовані політики аудиту;
- захист даних: шифрування даних для конфіденційних документів Microsoft Office за допомогою автоматичного застосування шифрування з використанням служб управління правами Windows (Rights Management Services, RMS).

За допомогою комбінації технологій DAC, AD RMS і FCI можна створювати потужні схеми управління доступом до документів і захисту конфіденційної інформації, реалізовуючи повноцінну систему DLP (Data Loss Prevention) на базі інфраструктури Windows Server 2012.

Науковий керівник – Б.Я.Корнієнко, к.т.н.,доц.

УДК 00:45:004.056.5 (043.2)

Ничипорук Р.Я.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ПРОГРАМНИХ ЗАСОБІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ (НСД)

У наший час розвиток інформаційних технологій сприяє прискоренню для створення та використання нових засобів та способів у сфері інформаційної безпеки. Активно розробляються платформи та програмні коди для апаратного, програмно – апаратного та програмного комплексу. Проаналізувавши статистику використання методів захисту, виявилось , що програмний комплекс являється більш розповсюдженим, адже інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

За допомогою спеціалізованого програмного забезпечення (ПЗ) можна забезпечити цілісніть, конфіденційність та доступність інформації від його редагування, копіювання та інших не правочинних дій, якій можуть нанести збитки та витік конфіденційних інформаційних ресурсів.

Метою захисту інформації є: обмеження фізичного доступу користувачів до автоматизованих систем (АС), ідентифікація та автентифікація користувачів, криптографічний захист, контроль цілісності, мережевий захист та інших засобів.

Одним з ключових методів захисту інформації від несанкціонованого доступу до каталогів чи файлів, являється розмежування повноважень та прав доступу користувачів до ресурсів АС.

Робота з системними життєво важливими файлами системи, а саме їх перейменування, видалення та створення копій файлів чи каталогів можуть призвести до значних змін в роботі програмного комплексу.

В ході роботи був розроблений програний продукт, який дозволяє захистити теку від НСД. ПЗ блокує правила на зміни атрибутів файлу для певних користувачів. Вибравши теку, необхідно добавити користувачів згідно так званих «чорних» списків. Для користувачів списку вибираються правила на редагування теки. Після чого користувачі списку немають права на зміни атрибутів файлу. Задля узгодженої роботи системи, адміністратор безпеки має правила на зміни всіх фалів та каталогів.

Розроблене ПЗ може використовуватися в АС-1 та АС-2. Робоча станція повинна підтримувати операційну систему (ОС) Windows 7 або Windows 8 з набором бібліотек не нижче NET.Framework 4.5. Розроблене ПЗ являє собою окремий додаток. Клієнтський запускається на кожному комп'ютері мережі, де планується проводити блокування каталогів та блокування несанкціонованих процесів.

Розроблена програма забороняє зміну атрибутів каталогів згідно заданого спику для заданих облікових записів в АС-1 та АС-2, що дозволяє забепечити високий рівень захщеності.

Науковий керівник – А.Б.Єлізаров, к.т.н.,доц.

УДК 004.056.5(043.2)

Карнацький О.С.
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

Із розвитком сучасних інформаційних систем зростає роль захисту інформації. Крім традиційних засобів криптографічного захисту для забезпечення таємності важливих даних використовується стеганографія. В залежності від переслідуваних цілей необхідно використовувати відповідні стеганографічні методи. Але іноді обрання контейнеру для приховування повідомлення з певних причин стає неможливим. В таких випадках для наявного контейнеру треба знайти оптимальний стеганографічний метод.

Мета дослідження – з'ясувати основні критерії вибору оптимального стеганографічного методу в залежності від заявленої цілі та при нав'язаному стеганоконтейнері, змінити який неможливо.

Як відомо, основними напрямками використання стеганографії є:

- прихований зв'язок, а саме - передача повідомлення таким чином, щоб інша сторона навіть не підозрювала про його існування;
- захист авторських прав, тобто вбудовування цифрових водяних знаків (ЦВЗ) для підтвердження авторства;
- прихована анотація документів шляхом внесення коментарів, що має бачити лише обмежене коло осіб, яким відомий ключ;
- завадостійка автентифікація, при якої стеганографічні методи використовуються разом із криптографічними, для запобігання реалізації атак на дані користувача.

В першому випадку метод обирається в залежності від декількох факторів, а саме: тип інформації, яка циркулює у системі передачі даних (у потенційного зловмисника не має виникнути підозр щодо повідомлення), об'єму повідомлення та важливості даного повідомлення (оскільки залежність ***[надійність стеганосистеми]/[об'єм повідомлення]*** має зворотно пропорційний характер).

В другому випадку вибір методу залежить лише від типу файлу, у який буде вбудовуватися ЦВЗ (найважливішим фактором у даному випадку є надійність ЦВЗ, тобто стійкість до викривлень).

В третьому ж випадку зазвичай мають справу із текстовими документами, і метод приховування обирається в залежності від розміру повідомлення.

В останньому випадку основним завданням є прихована передача даних користувача до приймальної сторони, тому метод обирається в залежності від рівня надійності, який він забезпечує.

Для кожного повідомлення, яке необхідно приховати, стеганографічний метод обирається індивідуально. Основними критеріями при виборі стеганографічного методу є: тип контейнера, об'єм повідомлення та надійність заповненого контейнера (стійкість до викривлень). Головний критерій обирається в залежності від поставленої цілі.

Науковий керівник – В.Г.Павлов, к.т.н., доц.

УДК 004.056.5(043.2)

Касапов А.Е.
Національний авіаційний університет, Київ

МАНДАТНИЙ КОНТРОЛЬ ДОСТУПУ В БАГАТОМАШИННИХ КОМПЛЕКСАХ

Значного прогресу зазнало впровадження примусового (мандатного) контролю доступу в операційних системах. Зокрема, програмний комплекс SELinux став поставлятися в офіційне ядро Linux вже декілька років. Однак розгортання даної технології є доцільним лише для одномашинного комплексу. Можливість міжсистемного та віддаленого керування ресурсами тільки починає з'являтися в SELinux, тому розширення інструменту керування політикою безпеки для багатомашинної системи є відкритим питанням.

У якості можливого вирішення цієї проблеми пропонується застосування централізованого управління безпекою багатомашинної автоматизованої системи із застосуванням мандатного контролю доступу SElinux та використання загальної політики безпеки. Даний спосіб реалізується за допомогою використання серверу керування політиками, виділеного сховища політик безпеки та серверу безпеки.

Сервер керування політиками містить блок генерації політик на основі шаблонів політик безпеки. Замість відтворення цілої політики у ручному режимі, генератор політик надає інструмент для їх автоматизованого створення за попередньо сформованими шаблонами (наборами суб'єктів, об'єктів та правами доступу у відповідності до певного програмного додатку). Для розподілу загальної політики між окремими елементами мережі сервер забезпечує механізм розбиття та доставки необхідних частин політики безпеки.

Розбиття політики відбувається відповідно до функціональних особливостей кожного з компонентів автоматизованої системи. Локальні менеджери безпеки, що встановлені на кожному елементі домену, звертаються за рішенням контролю доступу до серверу безпеки, який посилає запити до бази політик у режимі черги. Для зменшення кількості запитів сервер безпеки містить таблицю кешованих правил, за якими часто виконують запити.

Зазначена вище схема дає можливість позбавитися надлишкового використання ресурсів кожного вузла мережі завдяки усуненню непризначених для цільової системи правил політики безпеки. Разом з цим, більшість систем матимуть спільні класи об'єктів, такі як, socket, file, ipc та ін.

Для забезпечення цілісності загальної політики безпеки модель припускає механізм синхронізації усіх залежних частин загальної політики, розподілених між елементами автоматизованої системи.

Науковий керівник – Б.Я.Корнієнко, к.т.н.,доц.

УДК 004.627(043.2)

Курінь К.О.
Національний авіаційний університет, Київ

АЛГОРИТМ СТИСНЕННЯ-ВІДНОВЛЕННЯ ЗОБРАЖЕНЬ НА БАЗІ НЕСТАТИСТИЧНИХ МЕТОДІВ КОДУВАННЯ

Інформаційно-комунікаційні системи та мережі в сучасних умовах розвитку суспільства все ширше застосовують графіку різних класів, яка вимагає великих об'ємів пам'яті. Так, кожен піксел зображення кодується 24-ма бітами, стандартні зображення розміром 512×512 пікселів займатимуть 786432 байти, а зображення розміром 1024×1024 пікселів – 3145728 байт. Анімація, що також широко застосовується в комп'ютерних додатках, вимагає ще більшого об'єму пам'яті. Все це пояснює важливість використання сучасних технологій та методів стиснення.

З огляду на це мета наукового дослідження полягає в наступному: розробка алгоритму стиснення-відновлення зображень на базі методів кодування, відмінних від статистичних, з умов підвищення ефективності стиснення даних з одночасною мінімізацією спотворень у відновленому зображенні.

Наукова новизна дослідження полягає в наступному:

1. Розроблено алгоритм стиснення зображень на базі стандарту JPEG, який, на відміну від вказаного підходу: не використовує процедуру «укрупнення пікселів», яка є першопричиною появи артефактів у відновлюваному зображенні; враховує можливість використання алгоритму структурного кодування вмісту трансформант зображення замість алгоритмів статистичного кодування, що дозволяє досягти більшого ступеня стиснення при заданому рівні якості відновленого зображення.

2. Розроблено алгоритм структурного кодування трансформант зображення, що, на відміну від існуючих підходів: враховує доцільність розбиття вмісту квантованих трансформант на бітові шари замість представлення безпосередніми десятковими значеннями компонент; враховує можливість представлення бітових шарів трансформанти порядковими номерами розрахованими згідно методу кодування за кількістю бітових переходів; враховує можливість додаткового стиснення сформованих порядкових номерів з використанням методу RLE.

Практична цінність дослідження полягає в наступному:

1. Проведено оцінку якості відновлених зображень згідно значення пікового співвідношення сигнал/шум. Отримані результати дозволяють дійти висновку, що запропонований алгоритм вносить у відновлене зображення викривлення у допустимих межах чутливості людських органів.

2. Розраховано усереднений коефіцієнт стиснення для тестових зображень Запропонований алгоритм стиснення забезпечує виграш у ступені стиснення в порівнянні з існуючими методами: в 1,63 рази в порівнянні з алгоритмом JPEG для зображень з середнім ступенем кореляції; в 1,87 разів в порівнянні з алгоритмом JPEG для зображень з високим ступенем кореляції; в 1,39 рази в порівнянні з алгоритмом JPEG для зображень з дуже високим ступенем кореляції.

Науковий керівник – О.К. Юдін, д.т.н., проф.

УДК 004.056.52:57.087.1(043.2)

Лозицька Л.Г.
Національний авіаційний університет, Київ

ЗНАЧЕННЯ OPENSSH ДЛЯ БЕЗПЕКИМ МЕРЕЖІ

Безпека мережі важлива для захисту від атак, джерело яких знаходиться за її межами. Часто буває необхідно отримати доступ до комп'ютера віддалено. Якщо користувач відправляє логін і пароль у вигляді звичайного тексту, вони можуть бути перехоплені і використані зловмисником для отримання доступу до віддаленої системи від імені цього користувача. Комплект програм SSH забезпечує необхідний захист, шифруючи трафік, що передається, включаючи логін і пароль. SSH забезпечує безпечне з'єднання в небезпечній мережі, такій як Інтернет. OpenSSH це вільно поширювана заміна SSH, в якій були видалені всі патентозалежні алгоритми, всі відомі помилки з безпеки і додані нові можливості. У OpenSSH входить мережева служба sshd і три клієнтські додатки командного рядка (ssh - захищений клієнт віддаленого доступу до консолі; scp - захищена команда віддаленого копіювання; sftp - захищений псевдо-ftp клієнт, що дозволяє передавати файли інтерактивно).

Внаслідок проведеного аналізу OpenSSH можна сформувати список можливостей, завдяки яким варто використовувати саме OpenSSH:

- безпечна система аутентифікації; посилена система конфіденційності (всі канали зв'язку автоматично та прозоро зашифровані);
- безпечні X11-сеанси; довільний TCP/IP-порт може бути перенаправлений через захищений канал в обох напрямках;
- при RSA-аутентифікації клієнт перевіряє справжність сервера перед кожним новим з'єднанням;
- "Host authentication key" може використовуватися адміністрацією централізовано, а також створюватися автоматично при першому підключенні до машини;
- будь-який користувач може створити будь-яку кількість RSA-ключів для аутентифікації;
- на стороні сервера є свій власний RSA-ключ, який автоматично регенерується кожну годину;
- агент аутентифікації, що працює на ноутбуці чи Workstation користувача, може бути використаний для зберігання RSA-ключів;
- програмне забезпечення може бути встановлено та використано без root-привілегій;
- клієнт налаштовується за допомогою загальносистемних та користувацьких файлів конфігурації;
- додаткове стиснення всіх даних , що передаються у мережі за допомогою gzip, що може призвести до значного прискорення на повільних з'єднаннях;
- повна заміна функціональності rlogin, rsh та rcp.

Науковий керівник – О.О.Мелешко, доц.

УДК 004.056.52:57.087.1(043.2)

Підопригора Г.О.
Національний авіаційний університет, Київ

КРИПТОГРАФІЧНА СИСТЕМА ЗАХИСТУ LINUX

На сьогоднішній день жодна криптографічна система захисту інформації не може бути абсолютно надійною. Тому, для того щоб зробити неможливим перехоплення з незахищеної області пам'яті секретні паролі, криптографічні функції мають бути частиною операційної системи. В сімействі Windows, починаючи з Windows 95, забезпечується реалізація шифрування, генерації ключів, створення і перевірка цифрових підписів і других криптографічних задач. Ці всі функції необхідні для роботи операційної системи, однак ними може користуватися і будь-яка прикладна програма – для цього програмісту достатньо лиш звернутися до необхідної підпрограми так, як прописує криптографічний інтерфейс прикладних програм (CryptoAPI).

Розглядаючи Linux/Unix потрібно відмітити, що на даний момент в операційних системах типу Unix, на відміну від Windows, не існує єдиної системи криптографічного захисту. В них в залежності від ядра, використовують різні варіанти, але одними з найпоширенішими є :

1. cryptoloop + cryptoAPI (цей варіант є застарілим і більше не підтримується, але в ядрах гілки 2.4 його будуть ще довго використовувати). Його криптографічні уразливості поки що є некритичними, але від нього вже слід відмовлятися.
2. dm-crypt + cryptoAPI + cryptsetup. У нових ядрах 2.6 і нових дистрибутивах він дає готове шифрування.

a. LUKS - Linuxunifiedkeysetup - продовження і розширення проекту dm-crypt. Нові підходи в шифруванні, використання слотів з системою менеджменту ключів.

3. loop-aes. Альтернативна реалізація cryptoAPI для ядер 2.4 і 2.6. Інтеграція з GPG.

На сьогодні вбудована криптографічна система захисту Linux демонструє високий ступінь захисту, мінімум вірусів і як висновок - високу стабільність в роботі. Так як ця ОС поширюється по ліцензії GNU GPL, вона є безкоштовна і вільна, що дозволяє розробникам користуватися всіма її перевагами перероблюючи їх під свої цілі.

Отже, можна відмітити, що як Windows так і Linux в побудові криптографічної системи захисту використовують CryptoAPI.

Науковий керівник –О.О.Мелешко, доц.

УДК 004.735(043.2)

Поповкін В.В.
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ГЛОБАЛЬНИХ МЕРЕЖ

Сучасні неприривно змінні вимоги до телекомунікаційних систем зумовили необхідність появи нових технологій. В таких умовах постає невідкладне завдання побудування мережі, яка б відповідала принципово новим напрямкам інформаційного суспільства. Мережа наступного покоління – NGN (Next Generation Network) має на меті в найближчому майбутньому забезпечити суспільство додатковими інноваційними можливостями. За даними Міжнародного союзу електрозв'язку (МСЕ) впродовж 2015-2020 року відбудеться поступовий перехід до мережі майбутнього – FN (Future Network), необхідність якої пояснюється появою нових прикладних галузей, що дозволяють дистанційно керувати технікою.

Мережа майбутнього – це глобальна інформаційна інфраструктура (ГІІ), яка об'єднує у собі вже існуючі інформаційно-комунікаційні мережі з урахуванням компонентів, котрі тільки плануються до впровадження, з єдиним центром управління ГІІ, що здатна надавати повний спектр телекомунікаційних послуг на базі нових та інноваційних технологій. Для побудови мереж майбутнього планується використовувати кремнієві та оптичні технології, а швидкість передачі даних буде досягати 1 Тбіт/с. Також для мережі майбутнього повинна бути розроблена дуже гнучка архітектура та передбачене володіння властивостями безперервної адаптації до навколишніх вимог.

Мережа наступного покоління це результат неймовірних змін основних телекомунікаційних мереж, унаслідок яких різні функції, що стосуються послуг було відокремлено від технологій, пов'язаних з їх транспортуванням. Від мережі Інтернет мережа майбутнього відрізняється тим, що:

- являє собою відкриту мережу, яка утворилось шляхом приєднання мереж;
- має високу надійність та ступінь інтеграції;
- потребує значних додаткових інвестицій.

Перехід до NGN та FN має низку невирішених питань стосовно ціноутворення, захисту, надійності, але відкриває безліч можливостей для новаторських рішень, та в майбутньому може сприяти збільшенню доходів та прибутків. Мережа майбутнього буде здатна встановлювати бездротові, дротові та супутникові широкосмугові з'єднання, розширювати доступ по мережі Інтернет, скорочувати цифровий розрив та підвищувати ступінь проникнення зв'язку.

Отже, як безперечний висновок можна сказати, що розгортання мережі майбутнього це лише питання часу, адже реалізація FN дасть змогу надавати вільний доступ до інтелектуальних ресурсів у будь-який час і у будь-якому місці, гарантуючи високу якість і прийнятну вартість відповідних послуг.

Науковий керівник – Б.Я.Корнієнко, к.т.н., доц.

УДК 004.91 (477)(043.2)

Прокопенко А.А.
Національний авіаційний університет, Київ

СУЧАСНИЙ СТАН ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В УКРАЇНІ

Кожне підприємство, як суб'єкт економічної діяльності, повинно періодично надавати звіти до відповідних державних органів. Традиційна "паперова" форма звітності по-перше дуже незручна, а по-друге потребує суттєвих затрат часу, які зростають із збільшенням кількості звітуючих. Для створення сучасної системи листування та звітування 7 лютого 2002 року був прийнятий закон «Про електронні документи та електронний документообіг», у якому були закладені основні організаційно-правові засади електронного документообігу та використання електронних документів.

Мета дослідження – проаналізувати сучасний стан електронного документообігу в Україні, його основні складові, роль державних органів, які його забезпечують, та створити прогнози його подальшого розвитку.

Як важлива складова електронного документообігу розглядається електронний цифровий підпис, який виступає засобом підтвердження авторства електронних документів. Центри сертифікації ключів, виступають органами, що засвідчують електронні цифрові підписи.

Контроль Центрів сертифікації здійснюється двома уповноваженими державними органами: Міністерством юстиції України та Державною службою спеціального зв'язку та захисту інформації в Україні. Крім контролю системи електронного документообігу в Україні вони формують нормативну та правову базу, вимоги до основних елементів електронного документообігу та електронного цифрового підпису.

Для надійного захисту цілісності електронних документів повинні використовуватися спеціальні програмно-апаратні засоби формування цифрового підпису, котрі пройшли контроль та отримали сертифікат про відповідність усім вимогам, що викладені у нормативної документації.

У доповіді також буде розглянуто:

- правила оформлення сертифікатів;
- послідовність формування рівнів сертифікатів;
- склад пакету документів, що повинен надати замовник сертифікату;
- терміни дії сертифікатів різного рівня;
- процедура отримання сертифікатів фізичними особами та підприємствами;
- відповідальність за компрометацію сертифікатів;
- процедури анулювання та відкликання сертифікатів.

В Україні набуває поширення електронний документообіг, який зараз існує паралельно з традиційним "паперовим".

Науковий керівник – В.Г.Павлов, к.т.н., доц.

УДК 004.056.5(043.2)

Ревтюх В.С.
Національний авіаційний університет, Київ

ЗАСТОСУВАННЯ ДЕМІЛІТАРИЗОВАНОЇ ЗОНИ В КОМП`ЮТЕРНИХ СИСТЕМАХ

Демілітаризована зона (ДМЗ) являє собою конфігурацію брандмауера для забезпечення захисту локальних мереж. Сучасні методи розміщення даних на резидентному комп'ютері в ДМЗ використовують відкриття порту в брандмауері між комп'ютером в ДМЗ та внутрішньою мережею. Це створює загрозу безпеці та призводить до значної кількості помилок в налаштуванні брандмауера.

Сценарій, при якому інформація повинна бути передана на резидентний комп'ютер в ДМЗ - це розкриття даних для доступу з Інтернету. При реалізації ДМЗ в якості резидентних комп'ютерів можна використовувати віртуальні машини, які можуть існувати без зв'язку з внутрішньою мережею. Такий спосіб ефективний з точки зору безпеки, але не допускає передачу даних між внутрішньою мережею і резидентними комп'ютерами в ДМЗ.

Існують системи і методи, що забезпечують ІБ комп'ютера в ДМЗ, який не може підключитися до внутрішньої мережі, але при цьому здатний передавати дані з ДМЗ та на нього. Механізм включає в себе передачу файлів з віртуальних жорсткий дисків між внутрішньою мережею та головним комп'ютером.

Головний комп'ютер в ДМЗ може бути налаштований з двома мережевими картами. Один мережевий інтерфейс може бути підключений до мережі ДМЗ. Другий може бути підключений до внутрішньої мережі. Віртуальні машини можуть бути підключені тільки до адаптера ДМЗ. Фізичний хост може обмінюватися даними тільки з внутрішньою мережею.

Щоб передати дані в комп'ютер, розташований в ДМЗ, файл з віртуального жорсткого диска може бути скопійований на хост ДМЗ через внутрішню мережу. Резидентний віртуальний комп'ютер в ДМЗ може визначити наявність нового диска і встановити його. Через відсутність мережевого з'єднання між резидентними комп'ютерами в ДМЗ і внутрішньою мережею, передача файлів може відбуватись без будь-яких маніпуляцій в брандмауері.

Комп'ютерні інструкції, такі як програмні модулі, також можуть бути використані. Взагалі, програмні модулі включають процедури, програми, об'єкти, компоненти, структури даних і т.д., які виконують конкретні завдання або реалізації зокрема абстрактних типів даних. Розподілені комп'ютерні середовища можуть використовуватися там, де завдання виконуються за допомогою дистанційного пристрою обробки, які пов'язані через комунікаційні мережі або інші середовища передачі даних. У розподілених обчислювальних середовищах, програмні модулі та інші дані можуть бути розташовані як в локальному так і віддаленому комп'ютерному носії, включаючи пристрої зберігання пам'яті.

Науковий керівник – Б.Я.Корнієнко, к.т.н.,доц.

УДК 004.056.5(043.2)

Сніжко В.В., Корнієнко Б.Я.
Національний авіаційний університет, Київ

СПІЛЬНЕ ВИКОРИСТАННЯ МОДЕЛЕЙ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

Моделі безпеки відіграють важливу роль у процесах розробки і дослідження захищених комп'ютерних систем, тому що забезпечують системотехнічний підхід, що включає вирішення наступних найважливіших завдань:

- Вибір і обґрунтування базових принципів архітектури захищених комп'ютерних систем, що визначають механізми реалізації засобів і методів захисту інформації;
- Підтвердження властивостей (захищеності) систем шляхом формального дотримання політики безпеки (вимог, умов, критеріїв);
- Складання формальної специфікації політики безпеки, як найважливішої складової частини організаційного та документаційного забезпечення розроблюваних захищених комп'ютерних систем.

У реальних автоматизованих системах рідко зустрічаються системи захисту, орієнтовані виключно на забезпечення конфіденційності або виключно на забезпечення цілісності інформації. Як правило, система захисту повинна поєднувати обидва механізми - а значить, при побудові та аналізі цієї системи буде необхідним спільне використання декількох формальних моделей безпеки.

Розглянемо як приклад можливі варіанти спільного використання моделей Белла-ЛаПадули і Біба:

1. Дві моделі можуть бути реалізовані в системі незалежно одна від одної. В цьому випадку суб'єктам та об'єктам незалежно присвоюються рівні секретності та рівні цілісності.
2. Можливо логічне об'єднання моделей за рахунок виділення загальних компонентів. У випадку моделей Біба і Белла-ЛаПадули таким загальним компонентом є порядок розмежування доступу в межах одного рівня секретності.
3. Можливе використання однієї і тієї ж решітки рівнів, як для секретності, так і для цілісності. При цьому суб'єкти та об'єкти з високим рівнем цілісності будуть розташовуватися на низьких рівнях секретності, а суб'єкти та об'єкти з низьким рівнем цілісності - на високих рівнях секретності.

Формалізація механізмів захисту може переслідувати різні цілі, але головна з них - це оцінка стійкості архітектури реальних систем, що проводиться, наприклад, в рамках комплексного аналізу їх захищеності.

УДК 004.056.53(043.2)

Соловей Р.С.
Національний авіаційний університет, Київ

БЕЗПЕКА ІНІЦІАЛІЗАЦІЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ШЛЯХОМ СТВОРЕННЯ ДОВІРЧОГО МІКРОПРОГРАМНОГО СЕРЕДОВИЩА

Безпеку сучасних комп'ютерних систем неможливо забезпечити тільки шляхом установки захищеного операційного середовища та / або зовнішніх засобів захисту інформації. Це пов'язано з тим, що існують методи злому і шкідливі програми, що дозволяють впровадити зловмисний код до завантаження операційної системи, та тим самим відключити або знешкодити механізми безпеки. Через це захист на рівні операційної системи стає неефективним, оскільки він може бути зруйнованим ще на стадії завантаження BIOS. Для вирішення цієї проблеми найчастіше використовуються апаратні модулі довіреного завантаження операційної системи, але якщо шкідливому коду вже вдалось впровадитися у саму програму BIOS, то виникає можливість обминання команд передачі управління цього модулю програмними засобами. Також існує інший суттєвий недолік апаратні модулі довіреного завантаження - такі системи в принципі не підтримують віртуальне операційне середовище, в якому доволі часто працюють користувачі.

Тому заслуговує уваги розгляд інших шляхів створення довірчого мікропрограмного середовища та забезпечення цілісності та безпеки ініціалізації операційної системи, в тому числі віртуальної. Суть пропозиції полягає у доповненні програми BIOS, яка, як звісно, здійснює первинне завантаження комп'ютерних систем, власними модулями, за допомогою яких буде виконане блокування будь-яких змін програми BIOS в майбутньому без відому користувача.

Якщо розглядати процес завантаження операційного середовища як послідовність певних фаз, то важливо з'ясувати, коли відбувається виконання вбудованих модулів та від чого це залежить.

Проведені дослідження показали, що якщо модуль ініціалізації стандартний, то він більше залежить не від розробника материнської плати, а від версії ядра BIOS. Так у досить поширених версіях ядер BIOS AWARD v 4.51, v 6 та AMI v 8, модифікацію можна виконати під час фази 0 за рахунок використання механізму відновлення.

Таким чином, реалізація програмного засобу довіреного завантаження, побудованого на описаних вище принципах, має низку переваг, а саме:

- забезпечує необхідний рівень безпеки комп'ютерних систем, шляхом виключення вразливостей передачі управління, властивих апаратним засобам;
- забезпечує довірене завантаження віртуальних машин, що істотно знижує можливість створення середовища зловмисника в складних інформаційно-обчислювальних комплексах;
- використання програмного засобу має економічну перевагу оскільки не вимагає придбання спеціального електронного модулю.

Науковий керівник – В.Г.Павлов, к.т.н., доц.

УДК 004.056:004.415.5(043.2)

Стародуб Ю. І.
Національний авіаційний університет, Київ

ФАЗЗЕРИ ФОРМАТУ ФАЙЛУ

Існує чимало засобів фаззінгу, серед яких фаззери мережевого протоколу, формату файлу та інші. Зважаючи на це виникає актуальна задача в аналізі наявних фаззерів, зокрема фаззерів формату файлу, які мають свої переваги й недоліки**..**

Для класифікації фаззерів формату файлу було взято сукупність параметрів: вхідні параметри, вихідні параметри, метод фаззінгу, реалізація фаз фаззінгу, тип вхідних даних, мова реалізації та платформа, доступність використання, можливість відтворення виняткової ситуації.

Вхідні параметри – вхідні дані, які подаються фаззеру на початку експерименту.

Вихідні параметри – дані, які видає фаззер наприкінці експерименту.

Метод фаззінгу – метод створення вхідних експериментальних даних (мутаційний або породжуючий).

Реалізація фаз фаззінгу – можливість реалізації наступних фаз фаззінгу: визначення цілі, визначення вхідних значень, генерація(породження) некоректних даних, виконання некоректних даних, моніторинг виключень, визначення працездатності.

Тип вхідних даних – введення з інтерфейсних пристроїв; параметри програмного середовища; параметри командного рядка; комунікаційні протоколи; файли; дані в оперативній пам'яті.

Мова реалізації та платформа – мова програмування, на якій було написано даний засіб фаззінгу та операційна система, яка підтримує використання даного засобу.

Доступність використання – якісна оцінка зручності використання фаззера.

Можливість відтворення виняткової ситуації – незмінність експериментальних даних при повторному експерименті.

В ході даної роботи було проаналізовано більше десятка засобів фаззінгу формату файлу за відібраними параметрами. А саме: MiniFuzz, FileFuzz, SPIKEfile, notSPIKEfile, ZZUF, Intent Fuzzer, fsfuzzer, Ffuzzer, FileH, FileP.

В ході даної роботи було розглянуто фаззери формату файлу та проведено їх порівняльний аналіз. Результати проведеної роботи будуть корисні фахівцям при виборі засобу фаззінгу.

Науковий керівник – О.Г.Корченко, д.т.н., проф..

УДК 004.056.52:57.087(043.2)

Федоров Р.В.
Національний авіаційний університет, Київ

АНАЛІЗ ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СИСТЕМ РОЗПІЗНАВАННЯ ОСОБИСТОСТІ ЗА ГОЛОСОМ

Широке застосування інформаційних технологій призвело до загострення проблеми захисту інформації, що головним завданням має забезпечення цілісності, доступності та конфіденційності даних.

На сьогоднішній день одним з найкращих рішень є використання біометричних технологій (систем) контролю доступу, які мають достатньо високий ступінь надійності та займають гідне місце на ринку.

Біометричні системи (БС) використовують статистичні та динамічні характеристики користувачів (власників) інформаційних ресурсів, доступ до яких обмежується.

Мета роботи – проаналізувати біометричні системи розпізнавання голосу, виявити переваги та недоліки даних систем, розробити рекомендації щодо їх оптимального використання.

Розпізнавання за голосом (спектральний аналіз голосу) відрізняється від інших БС тим, що використовує акустичну інформацію, а не зображення. Головними факторами, які впливають на формування людської мови, є фізіологічні особливості, такі як голосові зв`язки, носова порожнина, форма та розмір губ тощо. Головною перевагою системи розпізнавання голосу над іншими БС є можливість передавати голосові дані дистанційно, наприклад, використовуючи телефоні лінії. Процес перевірки відбувається зі швидкістю вимови слів.

Метод розпізнавання голосу використовує три типа верифікації об'єкта мовлення: текст залежний, текст запиту та текст незалежний.

Слід зазначити, що даний метод є найбільш звичним для людини, має невисоку вартість, явною перевагою є його безконтактність.

До недоліків даного методу можна віднести високу чутливість до завад, що викликає необхідність наявності спеціалізованого завадоїзольованого приміщення; можливість перехоплення фрази; високий рівень помилок 1-го і 2-го роду. Якість розпізнавання залежить від багатьох факторів, таких як інтонація, швидкість мовлення, фізичний та психологічний стан джерела тощо.

У результаті аналізу ефективності розпізнавання особистості за голосом з'ясована неможливість забезпечення надійного рівня захисту інформації на базі тільки єдиного методу. Поєднання різних БС є найкращим рішення для контролю доступу, оскільки кожний метод окремо має як свої недоліки, так і переваги, а при використанні мультимодальних методів загроза мінімізується. Щодо системи розпізнавання голосу, то ідентифікацію джерела слід проводити з мінімальним рівнем шуму, для чого створювати відповідні умови, оновлювати базу шаблонів та удосконалювати систему.

Науковий керівник –О.В.Дубчак, ст.викладач