Міністерство освіти і науки України
Національний авіаційний університет
Інститут інформаційно-діагностичних систем
Кафедра засобів захисту інформації

ЗБІРНИК ТЕЗ

науково-практичної студентської конференції
«ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

5-6 березня 2015 р.

Київ

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ:

Голова:

Філоненко С.Ф.	д.т.н., професор, директор Інституту інформаційно - діагностичних систем Національного авіаційного університету

Члени:

Павленко П.М.	д.т.н., професор, заступник директора Інституту інформаційно-діагностичних систем з наукової роботи Національного авіаційного університету
Козловський В.В.	д.т.н., професор, завідувач кафедри засобів захисту інформації Національного авіаційного університету
Куц Ю.В.	д.т.н., професор, завідувач кафедри інформаційно – вимірювальних систем Національного авіаційного університету
Синєглазов В.М.	д.т.н., професор, завідувач кафедри авіаційних комп'ютерно – інтегрованих комплексів Національного авіаційного університету
Приставка П.О.	д.т.н., професор, завідувач кафедри прикладної математики Національного авіаційного університету
Юдін О.К.	д.т.н., професор, завідувач кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету
Корченко О.Г.	д.т.н., професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету
Конахович Г.Ф.	д.т.н., професор, завідувач кафедри телекомунікаційних систем Національного авіаційного університету
Щербак Л.М.	д.т.н., професор кафедри інформаційно-вимірювальних систем Національного авіаційного університету
Рєзніков М.І.	к.т.н., доцент, завідувач кафедри радіотехніки та радіоелектронних систем Київського національного університету імені Тараса Шевченка
Розорінов Г.М.	д.т.н., професор, завідувач кафедри систем захисту інформації Державного університету телекомунікацій
Власюк Г.Г.	д.т.н., професор, завідувач кафедри звукотехніки та реєстрації інформації Національного технічного університету України «КПІ»
Темніков В.О.	к.т.н., доцент кафедри засобів захисту інформації Національного авіаційного університету
Хлапонін Ю.І.	к.т.н., с.н.с. кафедри засобів захисту інформації Національного авіаційного університету

Секретар:

Краснопольський А.О.	к.т.н., доцент кафедри засобів захисту інформації Національного авіаційного університету

ЗМІСТ

УДК 654.924

О.С. Петров

Національний авіаційний університет
Petros.sanch@yandex.ua

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ СПОВІЩУВАЧІВ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

Сповіщувачі охоронної сигналізації, які застосовуються для виявлення руху в приміщеннях, що охороняються, відрізняються ціновими і технічними параметрами. Заявлені характеристики сповіщувачі руху повинні підтримувати протягом встановленого часу, що визначає їх безвідмовність в умовах різного роду завад. Тому ефективність сповіщувачів руху визначається: характеристиками виявлення, надійністю, завадостійкістю. Безумовно, ці показники залежать від випадкових факторів, чисельні значення яких оцінюються імовірнісними характеристиками.

Враховуючи якість надання інформації сповіщувачем і його ринкову ціну узагальнений показник ефективності сповіщувачів руху можливо виразити як співвідношення:

$$К_{max\,еф} = \frac{S}{C} = \frac{K_1 * Р_в + K_2 * Р_б + K_3 * Р_з}{\frac{C_i}{C_{max}}} \quad (1)$$

де, С – вага, як відношення ціни більш дешевого сповіщувача з гіршими характеристиками до ціни найбільш дорого сповіщувача руху із найкращими характеристиками;

К1, К2, К3 – вагові коефіцієнти по кожній із характеристик, які визначаються експериментально;

Рв, Рб, Рз – імовірності виявлення, безвідмовності, завадостійкості відповідно.

Для покриття вибраної зони охорони можливо використати дорогий сповіщувач з високою імовірністю виявлення або декілька дешевих сповіщувачів, які при сумісній роботі перекриють вибрану зону охорони. Імовірність виявлення дорогого сповіщувача - Pmin.

Для покриття зони охорони повіщувачами з гіршими характеристиками їх кількість n необхдно визначити за критерієм:

$$(1 - \prod_{i=1}^{n}(1 - P_{ві}){}^{n}) \geq P_{min} \quad (2)$$

Тоді коефіцієнт ефективності:

$$K_{сфф} = \frac{1 - \prod_{i=1}^{n}(1 - P_{ві})^{n}}{\sum_{i=1}^{n} C_i} \quad (3)$$

де Рві – імовірність вірного виявлення і-го сповіщувача;

Сі – ціна і-го сповіщувача;

і = 1, 2, …, n.

Якщо за вибраним критерієм провести розрахунки із врахуванням характеристик і ціни сповіщувачів, то з'явиться можливість оптимізувати кількість сповіщувачів і їхню ціну для зони охорони об'єкту.

Науковий керівник – доц., В.В. Литвин

УДК 004.032.26

Д.С. Бабак

Національний авіаційний університет, Київ
denisbabak1789@gmail.com

ХМАРНЕ ВІДЕОСПОСТЕРЕЖЕННЯ

Відеоспостереження на сьогодні є невід'ємною частиною систем безпеки. Зменшення вартості та збільшення якості відеокамер привертають увагу багатьох користувачів, але не кожен в змозі придбати необхідне обладнання, зробити правильні налаштування системи і обслуговувати її. Тому на ринку з'явилася нове рішення з використанням хмарних технологій (Cloud Computing, CC) - Video Surveillance as a Service (VSaaS) - хмарне відеоспостереження або «відеоспостереження як послуга». VsaaS надає сервіс для відеоспостереження, де клієнт, замість володіння повним програмно-апаратним рішенням, може вибрати конкретні послуги, наприклад, запис відео, розпізнавання позаштатних і підозрілих ситуацій та осіб, підрахунок людей на вході та інше.

Архітектуру хмари можна уявити, як спільну роботу серверів BackEnd і Front-End (вони відповідають за обробку відеопотоків, балансування навантаження, роботу з базами даних) і серверів додатків (вони надають зовнішнім програмам універсальні API).

В основі ПЗ для хмарних сервісів закладені три головні функції:

- Горизонтальне масштабування;
- Резервування;
- Балансування навантаження.

Головною перешкодою для розвитку VSaaS є недостатня пропускна спроможність каналів зв'язку за межами локальної мережі. Відеодані дуже об'ємні та враховуючи тенденцію до збільшення якості зображення та кількості камер, існуючі канали зв'язку можуть не впоратися з таким навантаженням. При цьому хмарні сервіси дуже чутливі до втрати навіть незначної кількості даних. Це може призвести до неправильного інтерпретації та обробки відеоданих.

Найперспективнішим на сьогодні способом зменшення об'єму даних, що передаються каналом зв'язку, є відеоаналітика. Проводячи аналіз відопотоку можна виділити пріоритетні дані, які згодом і будуть передані в хмару. Такий підхід дозволяє знизити навантаження на канали зв'язку в більш ніж 10 разів.

Пропонується наступний варіант роботи хмарного відеоспостереження з використанням відеоаналітики. Користувач створює в хмарі профіль, куди вноситься група камер, об'єднаних загальними правилами. У свою чергу, ця група може відноситися до ще однієї групи, з більш загальними правилами. Також для кожної камери є можливість створити індивідуальні налаштування.

Далі, коли камера підключається в хмару, встановивши TCP сесію, обробляються всі описані для неї правила (пріоритетними є більш вузькі правила) і створюється повний профіль камери. Профіль являє собою текстовий файл, де, на спеціальній мові описані правила і пріоритетність обробки відеоданих. По встановленому з'єднанню файл відправляється на камеру по HTTP або FTP. ПЗ

камери зберігає всі правила в свій конфігураційний файл і застосовує до отриманого зображення, виділяючи потрібні кадри і розраховуючи значення заданих змінних.

Після цього, камера встановлює два нових з'єднання в одному логічному каналі використовуючи протокол SSL. Перше з'єднання керуюче, друге - інформаційне. По керуючому з'єднанню передаються метадані, сформовані в результаті застосування всіх правил. Метадані являють собою інформацію про те, що прийде з інформаційного з'єднанню, як його потрібно обробляти і які процеси задіяти. За другим з'єднанню передаються фрагменти відеоданих відповідно до пріоритетів.

Таким чином, відеоаналітика розподіляється між камерою і хмарою. ПЗ хмари отримавши необхідні значення і кадри, застосовує алгоритми аналізу, зіставляє з попередніми результатами формує кінцевий відеопотік і при необхідності передає інші значення або тривожні сигнали.

Розглянутий механізм можна уявити, як математичні обчислення, де камера вибирає описані змінні, обчислює потрібні значення і передає їх у з'єднання, хмарне ПО аналізує отримані дані і видає кінцевий результат. Наприклад, користувач налаштував профіль камери стежити за повільними об'єктами в межах певного периметра. Камера підключається до хмари, і отримує конфігураційний файл, де описано на що і де звертати увагу, які параметри рахувати. Створивши друге підключення з двома сесіями, камера починає передавати по керуючому з'єднанню вирахувані значення швидкості, координат, пріоритети фрагментів та інше. По інформаційному передає фрагменти відео з описаними об'єктами. Програмне забезпечення хмари приймає ці значення і запускає процеси аналізу отриманих даних.

Хмарне відеоспостереження вже завоювало частину ринку, але більшість великих компаній зі складними системами і продовжують використовувати класичні системи. Враховуючи сучасний розвиток відеоаналітикі, збільшення обчислювальної потужності, поступової модернізації глобальних каналів зв'язку, можна передбачити в найближчому майбутньому широке поширення послуг VSaaS. У сфері безпеки разом з відеоаналітикою привабливим є моніторинг як послуга, це звільнить від додаткового штату співробітників. Також можлива інтеграція з вже існуючими системами безпеки. Зараз вже реалізуються проекти «безпечне місто» на базі хмарних технологій, там будуть об'єднані всі критично важливі міські структури. За послугами VSaaS майбутнє відеоспостереження, як і за більшістю хмарних сервісів.

Науковий керівник – к.т.н., с.н.с., Ю.І. Хлапонін

УДК 004.896:004.056.53

О.В. Стеценко

Національний авіаційний університет
oksanella@i.ua

МОДЕЛЬ НЕЧІТКОЇ НЕЙРОННОЇ ПРОДУКЦІЙНОЇ МЕРЕЖІ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання отримання узагальненої оцінки рівня захищеності інформації на основі методології, що враховує як кількісні, так і якісні показники оцінки.

Інформація про систему, її параметри, входи, виходи та стан системи може бути не надійною, не чітко визначеною та слабоформалізованою. Для оцінки захищеності інформації експерту необхідно враховувати всі можливі технічні канали витоку інформації, стан відповідного каналу буде відповідати стану захищеності інформації від певного виду загроз.

Для оцінки рівня захищеності інформації можуть бути застосовані нечіткі продукційні моделі та алгоритми нечіткого висновку на їх основі.

Нечіткі продукційні моделі є найбільш загальним видом нечітких моделей, які використовуються для опису, аналізу та моделювання складних, слабоформалізованих систем та процесів. Найчастіше вони основуються на алгоритмах нечіткої логіки Мамдані, Ларсена, Цукамото, Такагі-Сугено.

Незважаючи на безсумнівні переваги нечітких продукційних моделей їм притаманні і деякі недоліки:

- вхідний набір нечітких правил формулюється експертом і може виявитися неповним або таким, що має протиріччя;
- суб'єктивність в виборі виду та параметрів функцій приналежності в нечітких висловлюваннях правил;
- відсутність можливості автоматичного набуття знань.

Формально нечіткі продукційні моделі можуть бути представлені у вигляді нечітких продукційних мереж, які по своїй структурі ідентичні багатошаровим нейронним мережам, елементи кожного шару яких реалізують окремий етап нечіткого висновку в нечіткій продукційній моделі.

Структура нейромережевої системи (НМС) оцінки рівня захищеності інформації, яка представлена на рис. 1 включає m-нейронних шарів, які визначаються кількістю станів захищеності інформації відповідно до певного виду загроз. Стан захищеності відповідає нейронному шару, а число класів визначається параметрами, які визначаються та порівнюються з нормами з метою визначення стану захищеності інформації для кожного з визначених технічних каналів витоку згідно відпрацьованої моделі загроз для інформації.

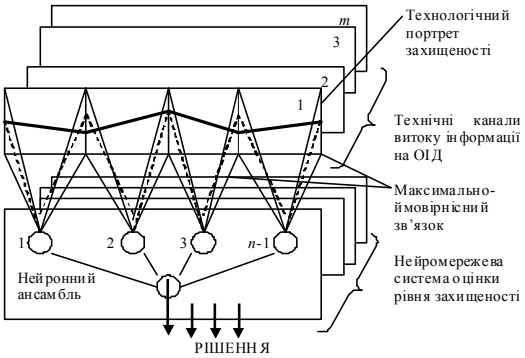

Рис. 1. Структура нейромережевої системи

Сукупність станів захищеності, які відповідають виявленим на об'єкті інформаційної діяльності технічним каналам витоку інформації в певний момент часу, може бути представлена у виді динамічних систем. Ці стани називаються подіями та представляються у виді технологічних портретів захищеності.

Середовище для НМС оцінки рівня захищеності інформації може бути представлено у виді сукупності дискретно-подійних систем із зв'язаними дискретними технологічними станами захищеності.

Отримуючи необхідну чисельність інструментальних вимірювань та спеціальних досліджень по кожному з технічних каналів витоку інформації, отриманих на ОІД, необхідно розробити таку процедуру обробки вимірювань, що дозволяє автоматично одержувати інформацію про технологічний стан захищеності кожного з каналів відповідно до затвердженої моделі загроз.

Висновки:

1. Оцінено моделювання системи оцінки рівня захищеності інформації на основі нечіткої нейронної продукційної мережі.

2. Нейромережева система дає можливість вирішування задачі оцінки рівня захищеності в масштабі часу, близькому до реального. Це досягається шляхом реалізації принципу паралельності обробки інформації в нейромережі.

Науковий керівник – к.т.н., с.н.с., Ю.І. Хлапонін

УДК 004.422

В.В. Кучинський

Національний авіаційний університет
Kuchinskiyvlad@gmail.com

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

Забезпечення заходів інформаційної безпеки (ІБ) стає все більш важливим питанням для багатьох банків. Усвідомлення масштабів можливих ризиків та загроз, а також вимог НБУ банки не тільки створюють письмову документацію

про комплексну політику інформаційної безпеки, але й забезпечують усім необхідним для ефективної роботи системи управління ІБ.

Правильний підхід до організації системи ІБ передбачає розмежування права на допуск, розуміння співробітників відповідальності за виток даних, своєчасне обновлення програмного забезпечення, контроль виконання всіх правил та інструкцій. При цьому ключовою задачею являється навчання персоналу інформаційної безпеки.

Для реалізації даної задачі широке застосування отримала DLP-система (англ.Data Loss Prevention). DLP-система повинна забезпечувати моніторинг поточного стану захисту й оповіщати про витоки, а також надати засоби активного аналізу вразливих місць і інструменти для швидкого розслідування інцидентів. Правильний вибір DLP-рішення залежить перед усім від розуміння, які ресурси потрібно захищати і де вони знаходяться.

Практично усі DLP-рішення в своїй основі містять технологію морфологічного аналізу даних. І цієї технології частіш за все достатньо для забезпечення захисту наявної інформації від витоку при відправленні поштових листів, месенджерів або публікацій у соціальних мережах. Більш складні системи включають у себе технологію цифрових відбитків або маркірування даних. Такі технології в поєднанні з морфологічним аналізом істотно підвищують безпеку конфіденціальної інформації.

Ефективне застосування технічних засобів захисту буде можливим тільки після реалізації наступних організаційних заходів:

- розробка політики інформаційної безпеки;
- аналіз загроз і оцінки ризиків;
- розробка критеріїв класифікації інформації;
- інвентаризація інформаційних ресурсів, котрі підлягають захисту.

Таким чином розгортання DLP-систем – достатньо складний процес, який потребує значних трудових затрат на початкових стадіях комплексу організаційних заходів, але впровадження DLP-системи виправдає усі затрачені ресурси.

Науковий керівник – к.т.н., доц., А.О. Краснопольський

УДК 621.38(075.8)

А.Ю. Шеремета

Национальный авиационный университет
Dron.andrew2011@yandex.ua

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ФИЛИАЛА БАНКА

Возрастающая роль информации, повсеместное внедрение и непрерывная работа по совершенствованию информационных технологий являются зачастую определяющими факторами формирования современного общества. При этом, для развитого и стабильного информационного общества характерным является:

с одной стороны, способность и возможность государства создавать условия для свободного доступа своих граждан к информационным ресурсам;

а с другой – умение защищать национальные информационные ресурсы, интересы личности, общества и государства в целом, от негативного как внутреннего, так и внешнего влияния, обеспечивая при этом не только надежное, но и безопасное функционирование и развитие национальной информационной инфраструктуры.

Эти свойства в своей совокупности составляют сущность информационной безопасности, что и определила, необходимость создания регуляторного механизма защиты информации. Где лицензирования, сертификации и государственная экспертиза, есть три основные составляющие.

Таким инструментом является «Комплексная система защиты информации». КСЗИ является глобальной концепцией безопасности и основой для безопасности инфраструктуры предприятия в целом.

Комплексная система защиты информации в банковском учреждении, является необходимым элементом всей банковской системы, так как подобные организации обрабатывают большой объем конфиденциальной информации, которую требуется защищать не только в коммерческих интересах самой организации, но и по требованиям законодательства. Банковские учреждения, являющиеся коммерческими предприятиями, имеют множество конкурентов, а конфиденциальная информация, обрабатываемая внутри предприятия, может дать конкурентное преимущество.

Научный руководитель – к.т.н., доц., Т.Л. Щербак

УДК 004.67(043.2)

С.В. Подгорний

Національний Авіаційний Університет.
meyers@bigmir.net

АНАЛІЗ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Система контролю доступу (СКД, іноді - система контролю та управління доступом - СКУД) - сукупність програмно-технічних засобів та організаційно-методичних заходів, за допомогою яких вирішується завдання контролю і управління відвідуванням окремих приміщень, а також оперативний контроль переміщення персоналу та часу його перебування на території об'єкта. Дійсно, СКД - це не тільки апаратура та програмне забезпечення, а продумана система управління персоналом.

Кожен співробітник, клієнт, відвідувач отримує ідентифікатор (електронний ключ) - пластикову картку або брелок з вмісту в ній індивідуальним кодом. "Електронні ключі" видаються в результаті реєстрації перерахованих осіб за допомогою засобів системи. В системі кожному коду поставлена у відповідність інформація про права власника картки. На підставі зіставлення цієї інформації і ситуації, при якій була пред'явлена картка, система приймає рішення: контролер

відкриває або блокує двері (замки, турнікети), переводить приміщення в режим охорони, включає сигнал тривоги і т.д. Всі факти пред'явлення карток та пов'язані з ними дії (проходи, тривоги і т. д.) фіксуються в контролері і зберігаються в комп'ютері.

На підприємствах можна виділити чотири характерні точки контролю доступу: прохідні, офісні приміщення, приміщення особливої важливості, і в'їзди / виїзди автотранспорту.

Складна система дозволить, крім обмеження доступу, призначити кожному співробітникові індивідуальний погодинний графік роботи, зберегти і потім переглянути інформацію про події за день. Системи можуть працювати в автономному режимі і під управлінням комп'ютера. Комплексні СКД дозволяють вирішити питання безпеки та дисципліни, автоматизувати кадровий і бухгалтерський облік, створити автоматизоване робоче місце охоронця. Набір функцій, які виконуються комплексними системами, дає можливість використовувати систему контролю для виконання конкретних завдань саме на Вашому підприємстві або об'єкті.

Науковий керівник — к.т.н., доц., В.А. Швець

УДК 621.391.(075.8.)

І.В. Івахіна

Національний авіаційний університет
ii-94@mail.ru

ОПТИМАЛЬНИЙ РОЗПОДІЛ РЕСУРСІВ В ДВОСТУПІНЧАСТІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

При формуванні системи захисту в інформаційній сфері, важливе значення має оптимізація показників. Одним із таких показників є кількість ресурсів, які виділяються на захист та їх розподіл між окремими об’єкти.

В банківській сфері об’єктами захисту є відділення банків. Під інформацією, яку необхідно захищати у відділеннях банку, можна вважати персональні дані клієнтів, інформацію про депозити, кредити, фізичних, юридичних осіб, інформація про рух коштів, прибутки клієнтів. Оптимізація розподілу ресурсів між окремими відділеннями, визначається їх вразливостями, а також кількість інформації на кожному з них. Останню величину можна визначити вважаючи кількість інформації пропорційної кількості клієнтів, або інакше кількості населення в зоні обслуговування.

Вразливості об’єктів описують дробово-лінійними функціями. Розв’язуючи задачу оптимізації для цільової функції, котра описує втрати інформації, можна знайти рішення поставленої задачі.

Суттю методу є максимізації за обмежених ресурсів. Умови задачі на оптимум і мету, яку треба досягнути, можна виразити з допомогою системи лінійних рівнянь. Невідомі в них тільки першого ступеня; жодне невідоме не перемножується на інше невідоме. В роботі розглядаються відділення банку Креді

Агріколь. Вразливості відділень та ймовірності нападу на кожне з них вважати однаковими. Оскільки вразливості, котрі залежать від співвідношення ресурсів нападу та захисту мають нелінійний характер, то розподіл ресурсів буде нерівномірним. Розраховано оптимальний розподіл ресурсів для двадцяти двох відділень банку, розташованих в Києві.

В роботі наведена методика розрахунку оптимального розподілу ресурсів між відділеннями банку, що сприятиме підвищенню економічних і технічних показників системи захисту інформації.

Науковий керівник — к.т.н., доц., Є.Г. Левченко

УДК 004.7.051

М.С. Молодець

Національний авіаційний університет
maksmolodetc@ukr.net

АУТЕРНЕТ ЯК ПОДАЛЬШИЙ РОЗВИТОК ІНТЕРНЕТУ

На сьогоднішній день більша частина людей просто не може уявити своє життя без Інтернету. Для когось це просто розвага, а для когось невід'ємна частина повсякденного життя і роботи. Але, якщо подивитися статистику, то виявляється, що доступ до Інтернету має всього лише 60% населення. А що ж робити іншим 40% людей. Відповідь на це питання вже існує. Звичайно ж, ця проблема буде вирішуватися не стандартними методами, так як, прокладати кабель на сотні кілометрів по важко прохідній місцевості або встановлювати щоглу мобільного зв'язку заради підключення декількох тисяч нових користувачів невигідно з економічної точки зору. Так от, вирішення цієї проблеми запропонувала некомерційна організація Media Development Investment Fund (MDIF), а конкретно директор компанії С. Карим. Нею запропонована ініціатива під назвою Outernet, яка вже в 2015 році, повинна забезпечити все населення планети безкоштовним доступом в Мережу. Планується розмістити на навколоземній орбіті безліч мініатюрних кубічних супутників супутниками CubeSats і з їх допомогою покрити мережею Wi-Fi всю земну кулю. Супутникова мережа буде працювати за кількома поширеними протоколами, включаючи DVB, Digital Radio Mondiale і багато адресні розсилки, що передаються по протоколу UDP. Тепер розглянемо за допомогою чого буде прийматися сигнал від міні-супутників CubeSats. Був розроблений прилад для прийому сигналу під назвою Lantern. Він постійно приймає радіохвилі, передані Outernet з космосу. Lantern може приймати і зберігати прийняту інформацію на своєму внутрішньому носії. Для перегляду контенту, що зберігається на Lantern, необхідно включити Wi-Fi точку доступу і підключитися до нього з будь-якого сумісного пристрою Wi-Fi. Кращий спосіб пояснити як працює Lantern, порівняти його з принципом роботи FM радіо:

Радіостанція використовує радіохвилі для передачі музики. Так само і Outernet використовує радіохвилі.

Радіо приймає сигнал. Радіо перетворює сигнал в музику, в той час як Lantern отриманий сигнал, перетворює в файли.

Радіо відтворює музику. Радіо дає інформацію за допомогою звуку, в той час як Lantern дає інформацію за допомогою Wi-Fi.

Ми чуємо музику. Наш телефон або інший включений Wi-Fi-пристрій „бачить "Lantern і дозволяє переглядати всі файли, які він отримав.

Раніше аналітики зробили припущення, що до 2033 року користувачі забудуть про слово„ інтернет ". Передбачається, що вихід в онлайн можна буде здійснювати через пральну машину або холодильник. Адже про існування телевізорів і фотоапаратів з можливістю підключення до мережі інтернет за наявності спеціального Wi-Fi-модуля ми вже знаємо і не дивуємося. Так що людство чекає ще багато цікавого у сфері інформатизації.

Науковий керівник: к.т.н., с.н.с. Ю.І. Хлапонін

УДК 004.032.26

С.О. Лановський

Національний авіаційний університет
toemylo55555@gmail.com

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ В СИСТЕМАХ ГОЛОСОВОЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

Все більшого розвитку набувають системи контролю доступу користувачів до певних ресурсів чи об`єктів. Також все більшого поширення набувають біометричні системи контролю доступу, що мають один головний показник – індивідуальну характеристику користувача, за якою надається право доступу. Однією з найменш досліджуваних тем в даній галузі є дослідження методу голосової ідентифікації людини з використанням нейронних мереж.

Мова - це послідовність звуків. Звук в свою чергу - це суперпозиція (накладення) звукових коливань (хвиль) різних частот. Хвиля характеризуються двома атрибутами - амплітудою і частотою. Для того, що б зберегти звуковий сигнал на цифровому носії, його необхідно розбити на безліч проміжків і взяти деяке «усереднене» значення на кожному з них.

Таким чином, механічні коливання перетворюються в набір чисел, придатний для обробки на сучасних ЕОМ.

Звідси випливає, що завдання розпізнавання мови зводиться до «співставлення» безлічі чисельних значень (цифрового сигналу) і слів з деякого словника (російської мови, наприклад).

Одним із методів реалізації систем ідентифікації людини за голосом є метод, заснований на використанні нейронних мереж.

При навчанні мережі з учителем можна навчити мережу розпізнавати об'єкти, що належать заздалегідь певному набору класів. Якщо ж мережа навчається без учителя, то вона може групувати об'єкти за класами відповідно до їх цифрових параметрів.

Таким чином, на базі нейронних мереж можна створювати навчаючу і самонавчаючу системи.

Можливість створення на базі штучних нейронних мереж самонавчаючихся систем є важливою передумовою для їх застосування в системах розпізнавання (і синтезу) мови, що дає змогу застосовувати такі системи для захисту приміщень від несанкціонованого доступу.

Нейронні мережі можна використовувати і більш високих рівнях розпізнавання злитого мовлення для виділення складів, морфем і слів.

У порівнянні з класичним програмуванням, коли алгоритм вирішення тієї чи іншої задачі задано жорстко, нейронні мережі дозволяють динамічно змінювати алгоритм простою зміною архітектури мережі.

Науковий керівник – к.т.н., доц., В.О. Темніков

УДК 621.396.962.2(043.2)

К.С. Кравченко

Національний Авіаційний Університет
katyuha14.11@mail.ru

НЕЛІНІЙНИЙ ЛОКАТОР

Нелінійні локатори (детектори напівпровідникових елементів) призначені для виявлення пристроїв несанкціонованого отримання інформації, встановлених в будівельних конструкціях, предметах меблів та інтер'єру.

Нелінійні радіолокатори характеризуються багатьма параметрами. Наприклад методом пеленгації, режимом роботи тощо.

Використання АФАР в якості антени нелінійного локатора дозволяє реалізувати різні режими сканування.

Локатор буде складатись з модулів. Це дозволити швидко замінити зламані частінити прилада, не відправляючі весь пристрій на ремонт, что дозволити зупинити роботу тільки на момент заміни модуля.

Рівносигнальний метод у порівнянні з амплітудними дозволяють підвищити точність вимірювання кутових координат, зменшити час вимірювання і досить просто здійснити автоматичне стеження за метою по кутових координатах.

Локатор працюватиме в неперервному режимі. Це дозволить позбутись впливу шумів, які є присутніми в імпульсному режимі.

Пристрій буде працювати на прийом другої та третьої гармоніки. Це дозволить оператору більш точно визначити, або ціль містить в своєму складі справжній напівпровідниковий елемент, або це фальшиве спрацювання на з'єднанням метал-оксид-метал.

Пристрій матиме можливість підключення до комп'ютера через інтерфейс USB 2.0. Підключення до комп'ютера забеспечує можливість перепрограмування нелінійного радіолокатора, перегляд результатів роботи на моніторі комп'ютера, настройку і тестування приладу.

На підставі всього написаного було прийнято рішення спроектувати в рамках даного проекту нелінійний локатор, що працює в постійному режимі, використовувати АФАР, рівносигнального метод пелінгації та підключення через інтерфейс USB 2.0.

Науковий керівник – к.т.н., доц., С.М. Скворцов

УДК 65.01

Р.И. Базюк

Национальный авиационный университет
brvr94@i.ua

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности.

Виды и цели аудита

Внешний аудит — это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Внешний аудит рекомендуется (а для ряда финансовых учреждений и акционерных обществ требуется) проводить регулярно.

Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании документа, обычно носящего название “Положение о внутреннем аудите“, и в соответствии с планом, подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации. Аудит безопасности информационных систем является одной из составляющих ИТ—аудита.

Целями проведения аудита безопасности являются: — анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС; — оценка текущего уровня защищенности ИС; — локализация узких мест в системе защиты ИС; — оценка соответствия ИС существующим стандартам в области информационной безопасности; — выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Научный руководитель – к.т.н., доц., Т.Л. Щербак

УДК 004.056.53

А.В. Яковлєв
Національний авіаційний університет, м. Київ
Yakovliev.A.V@gmail.com

КОМПЛЕКСНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ

Метою інформаційної безпеки є забезпечення безперебійної роботи організації та зведення до мінімуму збитків від подій, які становлять загрозу безпеці, за допомогою запобігання їм та зведення наслідків до мінімуму.

Нині питання побудови системи захисту є дуже актуальними та постійно ускладнюються. Це зумовлено стрімким розвитком сучасного ринку інформаційних та комп'ютерних технологій, засобів електронного обміну інформацією, засобів захисту інформації, а також засобів несанкціонованого отримання інформації. У зв'язку з цим з'явились та постійно вдосконалюються різноманітні технічні, програмні, організаційні та інші способи вирішення питань пов'язаних з побудовою комплексних систем санкціонованого доступу та питань, пов'язаних узагалі із захистом інформації загалом, незважаючи на її належність (державної, військової, комерційної, фінансової тощо).

Одним з найефективніших підходів до розв'язання задачі комплексної безпеки об'єктів різної форми власності є використання комплексних систем санкціонованого доступу.

Грамотна побудова та правильна експлуатація комплексних систем санкціонованого доступу на об'єкті дає змогу закрити несанкціонований доступ на його територію, в будівлю, окремі поверхи та приміщення. Водночас функціонування системи не спричиняє додаткових незручностей та перешкод для проходу персоналу та відвідувачів у дозволені їм для проходу зони.

Система контролю та керування доступом на об'єкті у наш час не усуває необхідності контролю з боку людини, але значно підвищує ефективність роботи служби безпеки. Це особливо важливо за умов наявності численних зон ризику на об'єкті з різним рівнем доступу. Комплексні системи санкціонованого доступу позбавляють охоронців від рутинної роботи із ідентифікації користувачів та надає їм додатковий час на виконання основних функцій: охорони об'єкта та захисту працівників та відвідувачів від злочинних посягань.

Оптимальне співвідношення людських та технічних ресурсів у такій системі вибирають відповідно до поставлених задач і мети та виявленого рівня можливих загроз. Зацікавленість в системах санкціонованого доступу останнім часом стрімко зростає у зв'язку з автоматизацією процесу ідентифікації та можливістю виконання системою багатьох додаткових функцій.

Розв'язання задач побудови комплексної системи санкціонованого доступу основується на двох складових: теоретичній (науковій) та практичній (отриманій на основі певного досвіду). Оптимальним є варіант, коли на основі певного теоретичного обґрунтування різноманітних варіантів розв'язання поставленої задачі будуть вироблені практичні рекомендації, які згодом будуть використані. Хоча на практиці досить часто все відбувається не завжди в такій послідовності. Є

багато випадків, коли практичні рекомендації та способи вирішення часто випереджають теоретичні. Якщо технічні рішення, які використовуються в деякій послідовності побудови комплексної системи захисту, не пов'язані єдиним системним проектом, не варто очікувати позитивного результату від реалізації окремих елементів системи. Отже, вирішуючи питання захисту інформації, неможливо обійтися без науково обґрунтованого комплексного підходу для розв'язання поставлених задач захисту, який би враховував різноманітні загрози, зокрема суспільству, установам, особистості тощо.

Науковий керівник – к.т.н., доц., Т.Л.Щербак

УДК 621.96(034.2)

Т.Б. Сава
Ю.С. Кравченко

Національний авіаційний університет
savochka.tan@gmail.com, ylua@i.ua

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Інформаційні системи обробки персональних даних (ІСОПД) за структурою є локальними інформаційними системами, які функціонують у складі корпоративних інформаційних систем. Вони складаються з програмних та апаратних засобів обробки інформації, а також мережевих каналів обміну даними. При цьому, досить часто, в якості каналу передачі даних між елементами системи використовується мережа інтернет. Така структура організації комп'ютеризованих систем обробки персональних даних (ПД), маючи суттєві переваги з точки зору вартісної складової побудови та експлуатації системи, передбачає необхідність впровадження ефективних систем захисту ПД, що обробляються системою, у відповідності до вимог чинного законодавства.

Виявлення потенційних загроз безпеці інформації та порушників інформаційної безпеки є обов'язковою умовою при розробці та впровадженні систем захисту інформації. До потенційних загроз інформаційній безпеці можна віднести наступні загрози.

Перехоплення даних. Наведений тип загрози може бути застосований у каналах передачі даних та бути направлений на незаконне використання інформації, спотворення та пошкодження її цілісності, а також на її несанкціоноване поширення.

Несанкціонований доступ до інформаційних ресурсів. Крім спотворення інформації, її копіювання, вилучення чи неправомірного поширення, такий тип загрози може нанести шкоду елементам інформаційної системи;

Загроза зі сторони штатних співробітників, які мають легальний доступ до ресурсів корпоративної інформаційної системи. Вилучення, знищення, спотворення та несанкціоноване поширення інформації може виникнути в результаті реалізації таких загроз;

Загроза втрати носія інформації та засобів її обробки. Загрози можуть бути спрямованими на знищення, спотворення, копіювання та неправомірне використання і поширення інформації.

Порушниками інформаційної безпеки і безпеки ПД, можуть бути як фізичні особи, так і організації. Таких порушників можна поділити на зовнішніх, до яких відносяться зловмисники які намагаються отримати доступ до інформаційних ресурсів, знаходячись поза межами захищеної інформаційної системи, та внутрішніх, які є легальними користувачами корпоративної інформаційної системи, в тому числі вони можуть бути і операторами ІСОПД. Загрози інформаційній безпеці можуть реалізовуватись внаслідок як навмисних так і ненавмисних дій внутрішніх порушників. Неуважність та некомпетентність оператора можуть бути причинами виникнення загроз безпеці інформації. Помста, матеріальна вигода, задоволення нездорових амбіцій – список можливих мотивацій навмисних дій зловмисників, які можуть привести до порушення цілісності конфіденційної інформації.

Приведені загрози інформаційній безпеці в повній мірі можна віднести і до ПД. При впровадженні систем захисту інформації при обробці ПД особливої уваги потребує попередження несанкціонованого поширення таких даних мережевими каналами, адже ПД передаються мережевими каналами і каналами інтернет. До таких каналів передачі даних вони можуть надходити як санкціоновано, так і несанкціоновано, внаслідок дій внутрішніх порушників. А отже системи попередження несанкціонованого витоку ПД мережевими каналами повинні розрізняти санкціоновані та несанкціоновані надсилання таких даних.

Науковий керівник – к.т.н., доц., Т.В. Німченко

УДК 004.422.83(043.2)

К.К. Казачанський

Національний авіаційний університет
kaka1193@mail.ru

РЕАЛІЗАЦІЯ АЛГОРИТМУ СКРЕМБЛЮВАННЯ У МОВІ ПРОГРАМУВАННЯ С++

Інформація є найціннішим ресурсом, тому її захист є пріоритетною задачею. В наш час, коли цінність інформації стає все вищою, а власники інформації хочуть як найбільше знизити ризик її втрати, розглядати цю тему в край необхідно. В країнах Західної Європи питанням захисту інформації приділяють не менше уваги ніж в нашій країні. Тому ця проблема актуальна на сьогодення як для користувачів телефонів та інших засобів передачі інформації, так і для її розробників. Згідно закону, захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Скремблер – програмний або апаратний пристрій (алгоритм), що виконує скремблювання - оборотне перетворення цифрового потоку без зміни швидкості передачі з метою отримання властивостей випадкової послідовності. Після

скремблювання поява «1» і «0» у вихідний послідовності різновірогідні. Скремблювання - оборотний процес, тобто вихідне повідомлення можна відновити, застосувавши зворотний алгоритм.

Пропонуэмий алгоритм скремблювання полягає в побітному обчисленні результуючого коду на основі бітів вихідного коду та отриманих у попередніх тактах бітів результуючого коду.

Після отримання заскрембльованої послідовності бітів приймач передає її дескреблеру, який відновлює вихідну послідовність на підставі співвідношення оберненого до того, яке використоввалось для скремблювання.

На ефективність скремблювання впливає багато факторів а саме: метод скремблювання , довжина фрагментів на які розбивається аудіо інформація, значення частот та їх кількість, відносно яких відбувається інверсія. Запропонований вище алгоритм скремлювання досить легкий у реалізації та може бути використаний для скремблювання аудіо інформації у кожному кадрі окремо.Недоліком даного алгоритму скремблювання є не надто високий рівень захисту аудіоінформації

Науковий керівник – к.т.н., с.н.с., Ю.І. Хлапонін

УДК 621.396.662.072.078(043.2)

Н. Р. Старинська
Д. М. Старинський
Національний авіаційний університет
starynska.natalia@gmail.com

ВПРОВАДЖЕННЯ СИСТЕМИ «БЕЗПЕЧНЕ МІСТО» ЯК КРОК ДО РЕАЛІЗАЦІЇ «БЕЗПЕЧНОЇ ДЕРЖАВИ»

Система забезпечення безпеки міста – інтегрована комплексна система, призначена для вирішення завдань забезпечення правопорядку, моніторингу, охорони власності та безпеки громадян у будь-якому куточку міста.

Основою технічної складової системи є створення системи моніторингу територій, об'єктів та транспортних комунікацій міста, включаючи контроль ввезення та переміщення особливо небезпечних речовин і предметів.

Безпечне місто - багатофункціональний, багатоцільовий нарощуваний комплекс, побудований на принципах інтегрованості, модульної та розподіленої архітектури, з використанням технологій інтелектуального аналізу даних.

Технічно система є сукупністю безлічі підсистем, об'єднаних єдиною транспортною середою і системою управління.

Система повинна забезпечувати спільну роботу підсистем моніторингу, оповіщення, інформаційної системи. При цьому обов'язковою є можливість як локального управління кожною з підсистем, так і можливість контролю та управління всією системою зі спільного центру. До складу системи обов'язково повинне входити глобальне сховище інформації. Крім того, система повинна

забезпечувати оперативний зв'язок диспетчерських зі всіма підрозділами, що забезпечують безпеку у місті.

Для вирішення завдань безпеки в масштабах міста необхідно модифікувати локальні центри моніторингу що вже існують і створювати нові сховища даних і центри управління, зводячи їх в єдину базу інформаційних ресурсів.

Система забезпечення безпеки міста створюється шляхом інтеграції інформаційних ресурсів з використанням єдиної мультисервісної цифрової мережі передачі даних.

Вузловими елементами системи є створені і створювані інформаційні та моніторингові системи, а також системи управління разом з вхідними що входять у їх склад джерелами інформації, підсистемами збору, зберігання, обробки і видачі інформації, підсистемами управління і користувачами систем.

Складовими автоматизованої системи забезпечення безпеки життєдіяльності міста є:

- єдина транспортна мультисервісна мережа;
- локальні вузли;
- центр управління доступом;
- територіально-розподілена структура джерел інформації;
- користувачі локальних вузлів;
- користувачі єдиної транспортної мультисервісної мережі;
- ситуативні центри.

Створюючи єдиний інформаційний простір, транспортна мультисервісна мережа об'єднує всю інформацію локальних вузлів, чергових частин, ситуативних центрів та центрального вузла доступу, а також надає можливість доступу до інформаційних ресурсів єдиної транспортної мультисервісної мережі, інших зацікавлених структур міста і центру.

Призначенням центру управління доступом є інтеграція всіх інформаційних потоків, що надходять від локальних вузлів та надання їх користувачам автоматизованої системи забезпечення безпеки життєдіяльності міста у відповідності до прав доступу.

Кожне звернення зовнішнього користувача до того чи іншого локального вузла супроводжується валідацією раніше виданих ключів тимчасового терміну дії на предмет аутентифікації сторін, що з'єднуються. Процесом видання, заміни та подовження повноважень ключів керує посвідчуючий центр.

Вирішуючи задачу інтеграції множинності інформаційних ресурсів, автоматизована система забезпечення безпеки життєдіяльності міста об'єднує на правах вторинних джерел інформації локальні вузли, що можуть розміщуватись на базі відомств та міських.

Ситуативні центри призначені для забезпечення і підтримки технології прийняття рішень керівництвом та фахівцями підрозділів структури міського управління в повсякденній діяльності, а також для запобігання або ліквідації наслідків критичних ситуацій у місті.

Основне завдання ситуативного центру — інформаційна підтримка на базі сучасних рішень технології ухвалення рішень керівництвом та фахівцями правоохоронних органів, органів міського управління.

Очікуваний ефект від використання системи:

– підвищення ефективності контролю над об'єктами інфраструктури міста і населенням
– підвищення рівня безпеки об'єктів інфраструктури і населення;
– підвищення ефективності та надійності контролю і управління транспортними засобами;
– підвищення ефективності рішення задач силових структур;
– недопущення і запобігання надзвичайним подіям неприродного характеру;
– підвищення ефективності заходів щодо ліквідації наслідків надзвичайних подій;
– забезпечення розвитку російських передових технологій і систем моніторингу на вітчизняній та зарубіжній елементній базі;
– стабілізація соціально-економічного розвитку міста;
– підвищення якості життя його населення;
– підвищення ефективності виконання завдань національною, економічною, екологічною і інших видів безпеки на рівні міста та держави в цілому.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.422

А.С. Комар

Національний авіаційний університет
komariiik@ukr.net

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ-ПРОВАЙДЕРА

Швидке знаходження корпоративної інформації - важливий чинник успіху любого інтернет-провайдера. Але найчастіше знайти корпоративну інформацію складніше, ніж в глобальній мережі. Розуміння особливостей корпоративного пошуку дозволяє правильно сформулювати вимоги до систем управління контентом (ECM). Особливості такого пошуку висвітлює інформаційний ресурс DOCFLOW.

Знаходження - це наука і мистецтво організації контенту в зручній для пошуку формі. Вона включає в себе не тільки функції пошуку, але й елементи для пошуку шляхом перегляду контенту та вилучення інформації.

Існують два основні підходи до пошуку: на підставі правил і статистичний. Ці два підходи можуть використовуватися самостійно, хоча в більшості сучасних систем вони доповнюють один одного.

Все розмаїття функцій, що забезпечують можливість пошуку, приховано від очей користувача. Найчастіше наявність таких можливостей підкреслюється як в поданні результатів пошуку, так і в стилі інтерфейсу. Тільки ретельно продуманий інтерфейс навігації буде ефективним і допоможе користувачеві знайти

інформацію. Безпека реалізується за допомогою вкладених рівнів деталізації, і надійна політика безпеки обов'язково підтримує спадкування.

Впроваджуючи засоби, що забезпечують знаходження, створюється ще два джерела контенту, які забезпечують специфічні заходи безпеки. Рішення, що забезпечує знаходження, генерує індекс або індекси і використовує їх для виконання своїх завдань. Якщо ці індекси не захищені від несанкціонованого копіювання, зчитування, зміни або знищення, вони легко можуть стати "чорним ходом" в систему. Навіть якщо у всіх інших відношеннях системи надійно захищені, то інформація буде вразлива для проникнення через впроваджений звичайний інтерфейс користувача. Згідно передовим методикам, у випадках, коли в рамках спільної роботи користувачі можуть надавати доступ до своїх запитів, здійснюється т.зв. "управління записом" в таких запитах, що запобігає зміні необхідних співробітникам запитів іншими користувачами. Можна виділити основні бізнес-стимули до впровадження технологій, що підвищують знаходження контенту:

- більш швидке і інформоване ухвалення рішень;
- підвищення оперативності реакції на зовнішні запити від клієнтів і партнерів;
- підвищення швидкості бізнес-процесів.

Знаходження є критично важливим елементом стратегії управління контентом. Функції доступу до інформації повинні допомагати користувачам знаходити документи та інформацію, які відповідають їхнім потребам. Якщо користувачі не можуть знайти контент, всі зусилля з його вилучення та зберігання, а також з управління цим контентом будуть марні. Таким чином, знаходження - це не просто можливість ввести текст у вікно пошуку і отримати результат. Мова йде про можливість виявити необхідну інформацію навіть якщо не знати точно, що саме потрібно шукати.

Науковий керівник – к.т.н., доц., А.О. Краснопольський

УДК 004.056.5

О.Д. Шиваков

Национальный авиационный университет
alex9@online.ua

НЕЙРОСЕТИ В СИСТЕМАХ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Эволюция средств обработки информации осуществляется в направлении создания систем информационных технологий с элементами самоорганизации, в которых присутствуют процессы зарождения, приспособления и развития. На названных процессах основаны биологические системы, для которых характерны опыт эволюции, селективный отбор. Заимствование архитектурных принципов биосистем привело к разработке теорий нейронных сетей, нечетких множеств, эволюционных методов, лежащих в основе искусственных интеллектуальных систем.

Применение нейронных сетей для решения задач защиты информации связано, в первую очередь, с интеллектуальным анализом и предсказанием временных рядов (например, динамики трафика защищаемой локальной сети), а также поиском скрытых закономерностей в массивах первичных данных посредством средств data mining and knowledge engineering.

В качестве генов выбираются значения весов связей, ассоциированные с входами формальных нейронов - группа весов, расположенная в отдельной строке матрицы весов, в качестве функции соответствия – обратная величина евклидова расстояния между расчетным и целевым значениями выходов, а в качестве генетических операторов - пересечение и мутация. Оператор пересечения создает пару дочерних хромосом из генетического материала обоих родителей путем обмена одноименными (случайно выбранными) генами, а оператор мутации в весе случайно выбранного гена хромосомы вызывает незначительное случайное изменение значения в заданном диапазоне. В каждом эволюционном цикле рассчитываются значения выходов нейронной сети и функции соответствия. Отбор хромосом в следующую популяцию производится с учетом функции соответствия. Затем производится следующая эволюционная попытка до тех пор, пока хотя бы одна из хромосом не удовлетворит требованиям по допустимой ошибке обучения нейронной сети.

Аналогичным образом генетические алгоритмы используют для оптимизации топологии нейронной сети, то есть числа нейронов и межнейронных связей в сети. Составляется матрица связей сети, каждый элемент которой отмечается нулем - если связь в нейронной сети отсутствует, либо единицей - в противном случае. Хромосома образуется путем последовательного соединения строк матрицы связей.

Как правило, эволюционный процесс включает в себя следующие этапы:

1. Задание размера популяции хромосом, вероятности выполнения операторов пересечения и мутации, число циклов обучения НС.
2. Выбор функции соответствия для процедуры эволюционного отбора (например, обратной величины евклидова расстояния между расчетным и целевым значениями выходовнейронной сети).
3. Выбор, в качестве начальной популяции, случайным образом сгенерированной совокупности хромосом.
4. Выбор одной из хромосом популяции и вычисление значения функции соответствия.
5. Действия по п. 4 повторяются для всей популяции хромосом.
6. Выбор (случайным образом), в соответствии со значением функции соответствия, пары хромосом и, применяя операторы пересечения и мутации, создание пары дочерних хромосом. Оператор пересечения, случайным образом, выбирает гены в родительских хромосомах и производит взаимный обмен генами, а оператор мутации, с низкой вероятностью (порядка 0,005), инвертирует один или два бита в случайно выбранном гене.
7. Формирование новой популяции путем включения в нее дочерних хромосом.

8. Действия по п.п. 6, 7 повторяются, пока размер новой популяции хромосом не достигнет размера исходной популяции.
9. Действия с п. 4 повторяются до тех пор, пока не сменилось заданное число популяций.

Генетические алгоритмы предоставляют собой эффективные средства оптимизации адаптируемых параметров интеллектуальных средств в составе системы защиты информации, в частности, взвешенных связей нейронной сети.

Научный руководитель – к.т.н., доц., В.А. Сердюков

УДК 004.056.5

В.С. Шпильовий
Київський національний університет імені Тараса Шевченка
Luthor_Lex@ukr.net

МЕТОДИ ПРОДИДІЇ ДИНАМІЧНИМИ СПОСОБАМИ ЗНЯТТЯ ЗАХИСТУ ПРОГРАМ ВІД КОПІЮВАННЯ

Серед методів протидії динамічним способам зняття захисту програм від копіювання викликають увагу перш за все наступні:

1. Періодичний підрахунок контрольної суми, області оперативної пам'яті яку займає образ задачі в процесі виконання. Це дозволяє: помітити зміни, внесені в завантажувальний модуль. У разі, якщо програму намагаються "роздягнути", виявити контрольні точки, встановлені відладчиком.

2. Перевірка кількості вільної пам'яті і порівняння і з тим обсягом, до якого задача "звикла" або "привчена". Ця дія дозволить застрахуватися від занадто грубого стеження за програмою за допомогою резидентних модулів.

3. Перевірка вмісту незадіяних для вирішення програми, що захищається, областей пам'яті які не потрапляють під загальний розподіл оперативної пам'яті, доступної для програміста, що дозволяє домогтися "монопольного" режиму роботи програми.

4. Перевірка вмісту векторів переривань на наявність тих значень, до яких задача "привчена". Іноді буває корисним порівняння перших команд операційної системи, що відпрацьовують ці переривання, з тими командами, які там повинні бути. Разом з попереднім очищенням оперативної пам'яті перевірка векторів переривань і їх примусове відновлення дозволяє позбутися від більшості присутніх у пам'яті резидентних програм.

5. Перевстановлення векторів переривань. Вміст деяких векторів переривань копіюється в область вільних векторів. Відповідно змінюються і звернення до переривань.

6. Постійне чередування команд дозволу і заборони переривання, що ускладнює установку відладчиком контрольних точок.

7. Контроль часу виконання окремих частин програми, що дозволяє виявити "зупинки" в тілі виконуваного модуля.

Багато з перерахованих захисних засобів можуть бути реалізовані виключно мовою Асемблер. Одна з основних відмінних рис цієї мови полягає в тому, що для нього не існує обмежень в області роботи зі стеком, регістрами, пам'яттю, портами вводу/виводу тощо.

Автокореляція становить значний інтерес, оскільки дає деяку числову характеристику програми. Ймовірно автокореляційні функції різного типу можна використовувати в тестуванні програм на технологічну безпеку, коли розроблену програму ще немає з чим порівнювати з метою виявлення програмних дефектів. Таким чином, програми мають цілу ієрархію структур, які можуть бути виявлені, виміряні і використані як характеристики послідовності даних.

Науковий керівник - к.в.н., доц., С.Я. Довбня

УДК 004.056.53 (043.2)

М.В. Шматько

Національний авіаційний університет
FN_SCAR@UKR.NET

ЗАСТОСУВАННЯ FUZZY-ТЕХНОЛОГІЙ ПРИ ПОБУДОВІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Світова економічна криза призвела до загострення конкурентної боротьби на світових ринках. В умовах глобалізації та наростаючої конкурентної боротьби комплексні системи захисту інформації (КСЗІ) як в комерційних організаціях так і в державних підприємствах та корпораціях України є досить пріоритетним питанням інформаційної безпеки держави. Все частіше виникає потреба створення надійного захисту та збереження інформаційних ресурсів, як на рівні всієї організації взагалі так і на рівні окремих її підрозділів. І часто в тому наскільки ефективним є КСЗІ залежить загальна конкурентоздатність всієї організації. Підвищення вимог до ефективності захисту інформації (СЗІ) супроводжується підвищенням вимог щодо ефективності використання фінансових ресурсів, що виділяються на захист інформації (ЗІ). На теперішній час, найбільше розповсюдження отримали два підходи до визначення оптимального варіанту побудови КСЗІ організацій. Перший з них ґрунтується на перевірці відповідності рівня захищеності інформації в організації вимогам одного зі стандартів (законодавчих актів) у галузі інформаційної безпеки. Основний недолік першого підходу полягає в тому, що коли рівень захищеності інформації чітко не визначений визначити найбільш ефективний варіант побудови КСЗІ організації достатньо складно. Другий підхід пов'язаний з використанням методів та моделей оптимізації складних систем для визначення оптимального варіанту побудови КСЗІ. У зв'язку з цим розробка відповідних методів та моделей оптимізації показників СЗІ отримує особливу актуальність. Кінцевою метою при оптимізації показників КСЗІ є забезпечення необхідного рівня інформаційної безпеки організації за різних умов конкурентної боротьби. Завдання ускладнюється тим, що пошук доводиться вести в умовах невизначеності, коли дії суперника нам не

відомі і, в кращому разі, можуть бути оцінені з певною долею ймовірності. При відсутності статистичних даних, що характерно для комерційних структур, вибір параметрів розрахунку і функціональних залежностей, які входять в математичну модель, ведеться на основі експертних оцінок і вимагає розробки відповідних методів та методик. Рішення зазначених задач потребує включення до складу процедур спеціальних оптимізаційних моделей котрі встановлюють залежність між показниками кінцевого ефекту функціонування системи і сукупністю її параметрів. Саме такий підхід може бути покладено в основу оптимізації систем захисту інформації в умовах інформаційного протиборства. Таким чином, задача побудови оптимальної комплексної системи захисту інформації може бути вирішена на основі теоретичного (системного) підходу котрий використовує усесторонній розгляд та врахування основних факторів які впливають на ефективність системи. Під дослідженням операцій розуміють застосування математичних кількісних методів для обґрунтування рішень у всіх областях цілеспрямованої людської діяльності.

Реальною альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації (КСЗІ) є застосування у дослідженнях Fuzzy-технологій, які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності. Вони уможливлюють аналіз значної кількості якісної інформації, отриманої від експертів та доповненої кількісними даними. Fuzzy-технології є сукупністю теоретичних основ, методів, алгоритмів, процедур і програмних засобів, що базуються на використанні теорії нечітких мір (ТНМ) і оцінок експертів для вирішення широкого класу задач з самих різних областей. Теорія нечітких мір, нечіткої логіки або Fuzzy Logic – новий підхід до опису процесів, в яких присутня невизначеність, що ускладнює і навіть виключає вживання точних кількісних методів і підходів. Основна відзнака методу – введення лінгвістичних змінних (суб'єктивних категорій) і методів їх обробки. Ця теорія може виступати як інструмент моделювання невизначеності, який базується на відомій розумовій здатності людини оперувати якісними категоріями і оформляти свої логічні висновки також в якісній формі.

Застосування даної технології підвищує достовірність і якість рішень, що приймаються, при суттєвому зниженні вимоги до вхідних даних (їх якості, кількості, достовірності), формалізація яких виконується настільки точно, наскільки дозволяє їх обсяг і якість. Розроблені моделі і методи вирішення задач нечіткого математичного програмування, які адекватні сучасним умовам функціонування спеціальних об'єктів інформаційної діяльносі (СОІД), дозволяють підвищити наукову обгрунтованість, ефективність рішення, що формулюється та приймається при нечіткій вхідній інформації, збільшують аналітичну базу, надають можливість формалізації різних параметрів задачі та різноманітних цільових установок.

Необхідно відзначити, що нечіткі числа багато в чому аналогічні розподілам теорії імовірності, але вільні від властивих останнім недоліків, а нечіткі описи є моделлю згортки окремих сценаріїв розвитку подій з одночасним зважуванням

цих сценаріїв за рівнем можливості (аналогічну функцію виконує і щільність імовірнісного розподілу).

Крім того, існує ще декілька причин використання ТНМ. По-перше, нечіткі множини ідеально описують суб'єктну активність посадової особи, що приймає рішення щодо введення КСЗІ в експлуатацію. По-друге, нечіткі числа ідеально підходять для планування факторів у часі, коли їх майбутня оцінка ускладнена (розмита, не має достатніх імовірнісних умов). Таким чином, всі сценарії за тими чи іншими окремими факторами можуть бути зведені в один сценарій у формі трикутного числа, де відокремлюють три позиції: мінімально можливе, найбільш очікуване та максимально можливе значення фактору. Причому ваги окремих сценаріїв у структурі зведеного сценарію формалізуються як трикутна функція приналежності рівня фактора нечіткій множині "приблизного рівняння середньому". По-третє, при використанні нечітких множин ми можемо в межах однієї моделі формалізувати особливості застосування СОІД.

Науковий керівник – к.т.н., доц., В.О. Темніков

УДК 623.537.531

В.О. Дуда

Національний авіаційний університет
Duda_Vasia@ukr.net

ЗАХИСТ ІНФОРМАЦІЇ ВІД ЗНИЩЕННЯ ЕЛЕКТРОМАГНІТНИМ ІМПУЛЬСОМ

Корінні зміни поглядів в останні роки на стратегію, тактику та цілі ведення бойових дій і війни в цілому збільшив інтерес до розробки, випробувань і застосування нових видів нетрадиційної зброї і в першу чергу електромагнітної зброї (ЕМЗ). Досвід випробувань, застосування, дослідження в даній галузі та аналіз перспектив розвитку показав, що вже в найближчий час ефективність її бойового впливу на особовий склад та техніку противника передбачається більшою ніж ядерних боєприпасів, зрозуміло коли мова йде про досягнення конкретних цілей війни, а не про стратегічне стримання.

Електронний вплив проявляється як електронний (тимчасовий) пробій компонентів РЕЗ.

Електричний вплив здійснюється за рахунок стрибків напруги джерел живлення (як первинних, так і вторинних). Цей фактор призводить до виходу із ладу запобіжників, пробоїв конденсаторів, трансформаторів, індуктивних дроселів та інших елементів, які мають реактивний опір.

Електромеханічний вплив полягає у створенні механічних сил за рахунок магнітного поля навколо провідників, а також механічних розривів через різну теплоємність елементів з'єднань.

Термофізичний вплив полягає у виникненні теплового (необоротного) пробою електронних компонентів різних типів і з'єднань в усіх системах, плавленні і

вигоранні металізації (контактних доріжок), а також у безпосередньому впливі на вибухові речовини.

Хімічний вплив полягає у зміні та порушенні хімічного складу речовин, які використовуються в елементах радіотехніки (електролітичні конденсатори, масляні потенціометри, системи стабілізації та гальмування, гідросистеми і т. ін.).

Тому в залежності від електромагнітної стійкості до зовнішніх ЕМВ усю чутливу до них апаратуру можна поділити наступні групи:

– напівпровідникові прилади (діоди, транзистори, інтегральні мікросхеми, у тому числі аналогові НВЧ ММІС (Monolithic Microwave Integrated Circuitry), тощо);
– електровакуумні прилади (радіолампи, магнетрони, клістрони, розрядники);
– мікроелектромеханічні системи (МЕМС, Micro-Electro-Mechanical System);
– електротехнічні пристрої (трансформатори, дроселі та інші, що мають реактивний опір);
– світлочутливі прилади та елементи (фоторезистори, світлодіоди, світловоди);
– електромеханічні (реле, електричні двигуни, електрозамки тощо);
– термоелементи (термореле, термодатчики);
– електрохімічні прилади (конденсатори, спіральні потенціометри, акумулятори);
– прилади комутації та монтажу (міжблочні проводи, шлейфи, джгути, друковані плати, роз'єми).

В сучасних умовах основним методом захисту, що заснований на відбитті (відводі) уражаючої енергії, всіх без виключно радіоелектронних приладів, електричних мереж та кіл, ліній зв'язку і автоматики, енергетичного обладнання та комп'ютерних мереж є екранування.

Екрануванням називається локалізація електромагнітного поля в певному просторішляхом обмеження його розповсюдження всіма можливими способами.

Найбільш поширений вид екрану – це металева замкнута оболонка, що перешкоджає попаданню електромагнітного поля в простір, зайнятий електронним пристроєм. Крім свого основного функціонального призначення екран виступає як елемент постійної конструкції і окрім ослаблення і поглинання енергії електромагнітного поля повинен володіти необхідною механічною міцністю, жорсткістю, зручністю закріплення в загальній конструкції приладу, мати мінімальні розміри і масу.

Тому вибір матеріалу екрану диктується з одного боку ефективністю захисту, а з іншого боку – виробничими умовами виготовлення (якщо ж екран використовується ще і як несучий елемент, то враховуються вимоги обумовлені і цією обставиною).

З фізичної точки зору екранування можна звести до наступного: хвилі електромагнітного поля частково відбиваються від зовнішньої поверхні екрану, частково поглинаються матеріалом екрану, а решта частини проходить крізь екран.

Тому створені такі пристрої захисту електричних мереж, як заземлення, захисні розрядники, гібридні фільтри, трансформатори і дроселі, роз'єднувачі та інші електромеханічні запобіжні пристрої, при використанні яких захист

здійснюється за допомогою виключно якогось з цих пристроїв або завдяки їх комбінування в єдину схему захисту.

Недоліками захисних розрядників є великий час спрацювання, роз'єднувачів – велика інертність та можливість використання в обмежених випадках, фільтрів, трансформаторів і дроселів – необхідність відводу енергії, і всіх без виключення вищезазначених приладів – низька стійкість до дії енергії ЕМІ приведених показників.

Всі ці прилади, що засновані на відбитті (відводі) уражаючої енергії електромагнітних хвиль, або як запобіжні роз'єднувачі, через велику енергетичну потужність і досконаліть нових видів зброї ЕМІ, не забезпечують повного знешкодження уражаючої енергії.

Таким чином, універсального захисту РЕЗ і кіл електрообладнання від зброї ЕМІ з точки зору забезпечення не тільки ефективного екранування всього об'єкта, але також захисту отворів (вводів), які існують через конструктивні і технологічні дефекти в екранах існує. Хоча теоретичних розробок, що присвячені фізичним, хімічним, енергетичним та іншим основам вивчення ЕМВ достатньо.

Науковий керівник – к.т.н., с.н.с., Ю.І. Хлапонін

УДК 004.93

В.С. Куценко

Національний авіаційний університет
Vetal0k@yandex.ua

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

Біометрія вже давно перейшла із розряду фантастики до розряду сучасних технологій, що набули нового, вужчого значення. Зараз під біометричними технологіями найчастіше розуміють автоматичні або автоматизовані методи розпізнавання особи людини за його біологічними характеристиками або проявами. Нині існують різні способи і методи біометричної ідентифікації, але вони базуються в основному на вимірюванні фізіологічних властивостей, а також особливостях поведінки особи. Серед них такі напрямки, як розпізнавання за геометрією руки і пальців, венозною структурою, райдужною оболонкою, внутрішньою структурою дна ока, рисами обличчя, відбитками пальців. Відомі спроби використання для цих цілей зовнішньої форми вуха, структури долоней і навіть запаху людського тіла.,

Біометричними називають документи, що посвідчують особу та містять електронний носій інформації, на якому записано інформацію про біометричні дані власника документу з метою його ідентифікації. Передбачається, що такі документи найбільш захищені від підробок та виключають можливість користування ними будь-якою особою, окрім власника. Головна ідея впровадження більш захищених документів, які забезпечують ідентифікацію особи - це суттєве підвищення захищеності суспільства від проявів злочинності та міжнародного тероризму.

Біометричні паспорти набувають все більшого поширення у світі. Відповідно до інформації всесвітньої організації цивільної авіації (ІСАО) більше 90 країн з 193 держав-членів ООН в даний час видають такі документи, при цьому ще більше двадцяти держав готові до впровадження таких документів в найближчі роки.

6 грудня 2012 року набрав чинності Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують гросмадянство України, посвідчують особу чи її спеціальний статус». Відповідно до цього Закону в Україні розпочато роботи із запровадження оформлення і видачі паспорта громадянина України, що містить безконтактний електронний носій із біометричними даними власника документу, в регіонах та інфраструктури його функціонування.З метою запровадження біометричних документів для виїзду за кордон Урядом прийнято Постанову від 7 травня 2014 р. № 152 "Про затвердження зразка бланка, технічного опису та Порядку оформлення, видачі, обміну, пересилання, вилучення, повернення державі, знищення паспорта громадянина України для виїзду за кордон з безконтактним електронним носієм, його тимчасового затримання та вилучення".Відповідно до зазначеної постанови, біометричні закордонні паспорти в Україні запроваджуються з 1 січня 2015 року.

Науковий керівник – д.т.н.,проф., В.В. Козловський

УДК 004.056.5:004.7 (043.2)

І.Ю. Петруняк

Національний авіаційний університет
kaknibud123@gmail.com

МОДЕЛІ АНОМАЛЬНОГО СТАНУ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Актуальність даної роботи полягає в тому, що несанкціоновані дії на ресурси інформаційних систем впливають на оточуюче середовище і породжують в ньому певні аномалії. Таке середовище зазвичай слабоформалізоване, нечітко визначене і для виявлення атак, що породили аномалії, в такому середовищі потрібно використовувати ефективні моделі і методи. Формалізувати і ефективно обробити інформацію в такому середовищі дозволяють методи і моделі теорії нечітких множин. У зв'язку з цим актуальним завданням при розробці засобів, що розширюють можливості сучасних СВВ є створення, на основі теорії нечітких множин, моделей, методів і систем виявлення аномалій, породжених мережевими кібератаками.

Наукова новизна полягає в наступному: на основі базової моделі параметрів, універсальної моделі еталонів і моделі евристичних правил розроблено метод виявлення аномалій, породжених діями неавторизованої сторони, який дозволяє на основі експертного підходу і сформованих нечітких поточних параметрів створювати засоби ідентифікації несигнатурного типу кібератак;

Дана робота має на меті розробку моделей і засобів ідентифікації аномального стану, для розширення можливостей системи виявлення несигнатурних типів кібератак в комп'ютерних мережах. Для досягнення поставленої мети необхідно вирішити такі основні завдання: дослідити сучасний стан розвитку теоретичної та практичної бази, що використовується для виявлення атак в комп'ютерних системах; розробити базову модель параметрів і універсальну модель еталонів для відображення та виміру аномального стану в оточуючому середовищі, характерного для певного типу кібератак в комп'ютерних мережах.

На основі базової моделі параметрів, універсальної моделі еталонів та моделі евристичних правил було розроблено метод виявлення аномалій породжених кібератаками в комп'ютерних мережах.

На основі отриманих результатів експлуатації даної моделі можна сказати, що дослідження сучасного стану теоретичної та практичної бази, яка використовується для виявлення атак в комп'ютерних системах, показали недосконаліть відповідних засобів безпеки щодо їх можливостей ідентифікувати в нечітко визначеному слабоформалізованому середовищі несигнатурного і нових типів кібератак. Використання методів і моделей нечітких множин для побудови засобів виявлення аномалій, породжених атакуючими діями, дозволить удосконалити існуючі системи виявлення вторгнень і шляхом контролю активності в оточуючому середовищі ідентифікувати небезпечні аномальні стани.

Науковий керівник – д.т.н.,проф., В.В. Козловський

УДК 004.056.53

О.Р. Гич

Національний авіаційний університет
ksliand1@googlemail.com

АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ЗАХИСТУ МОБІЛЬНИХ ТЕЛЕФОНІВ ВІД ВИТОКУ ІНФОРМАЦІЇ

На сьогоднішній день сучасні мобільні телефони це не тільки засоби зв'язку, а й багатофункціональні пристрої, які виконують безліч функцій, серед них створення фото і відео файлів, запис аудіо інформації на вбудований мікро-цифровий диктофон протягом чотирьох годин і більше, здійснювати передачу по радіо ефіру аудіо та відео інформації в реальному часі. Також за допомогою мобільного телефону можна здійснити прослуховування розмов

Мобільний телефон є складною мініатюрною приймально-передавальною радіостанцією. Найпростіше прослухати розмову, якщо один із абонентів веде бесіду із звичайного стаціонарного телефону, для цього, достатньо лише отримати доступ до розподільної телефонної станції. Складніше – мобільні переговори, оскільки переміщення абонента в процесі розмови супроводжується зниженням потужності сигналу і переходом на інші частоти у разі передачі сигналу з однієї базової станції на іншу. Захист мобільних телефонів здійснюється за допомогою різних методів, серед них найпоширенішими є використання криптографічних

систем захисту (скремблерів), односторонніх маскіраторів мовлення, засобів пасивного захисту, постановників активної загороджувальної перешкоди.

Для захисту мобільного телефону від прослуховування рекомендується: тримати документи з ESN-номером телефону в надійному місці; щомісяця і ретельно перевіряти рахунки на користування мобільним зв'язком; тримати телефон вимкненим до того моменту, поки не вирішили ним скористатися. Цей спосіб найпростіший і найдешевший, але слід пам'ятати, що достатньо одного виходу на зв'язок, щоб виявити MIN/ESN номер апарату; регулярно змінювати MIN-номер вашого апарату через компанію, що надає вам послуги мобільного зв'язку; встановити додатковий чотиризначний PIN-код, що набирається перед розмовою. Цей код ускладнює діяльність шахраїв, так як вони зазвичай перехоплюють тільки MIN і ESN номера, але невелика модифікація апаратури перехоплення дозволяє виявити і його. Отже, під час важливих переговорів, для уникнення витоку інформації, потрібно вимкнути телефон, витягнути з нього батарею.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 681.3.8

Е.Я. Серегин

Національний авіаційний університет
quadr1k@mail.ru

ЗАЩИТА ГОЛОСОВЫХ СОЕДИНЕНИЙ ОТ ПРОСЛУШИВАНИЯ

Прослушать чужие разговоры при передаче голоса по IP намного проще, чем в случае классической телефонии. Это утверждение касается и корпоративных сетей, но в первую очередь относится к соединениям через Internet. Конечно, для обеспечения конфиденциальности можно применять те же методы, что и при защите традиционной передачи данных, а именно — шифрование или VPN. Однако их внедрение должно отвечать специальным требованиям к качеству голосовой связи.

Сигнальные и голосовые пакеты необходимо изолировать. Для этого существует масса возможностей, выбор которых зависит от предполагаемой среды передачи — Internet, Intranet, Extranet, а также совместимость брандмауэров с VoIP и VPN.

Под Intranet понимают частную сеть IP, по размерам и покрытию сравнимую с классической телекоммуникационной системой. Если применяется единая сеть с концентраторами, то данные сигнализации, а также соответствующие голосовые данные доступны на каждом порту. Подслушивающее устройство или самопрограммируемый инструмент можно установить в любом месте сети и прослушивать все данные.

В общедоступной сети Internet пользователь практически не может влиять на маршрут пакета. Теоретически на любом узле необходимые пакеты можно скопировать. По сравнению с мультиплексорами и телефонными коммутаторами

для голосовой связи, узлы Internet защищены хуже. Хакеры уже взламывали их, после чего могли манипулировать всеми проходящими через узлы пакетами или копировать их. Кроме того, закон о телекоммуникациях требует, чтобы спецслужбы имели возможность прослушивания в рамках оперативно-розыскной деятельности.

Технология VoIP сама по себе достаточно незащищена и предоставляет множество возможностей для атаки. Однако в Intranet, да еще на базе коммутируемой сети, многие слабые места уже устранены. При помощи специализированного аппаратного шлюза VPN можно установить защищенную связь между офисами. Однако шлюз VPN не должен быть реализован в виде программного обеспечения на брандмауэре, поскольку в таком случае вариация времени задержки будет зависеть не только от нагрузки процессов VPN, но и от общего трафика данных.

Научный руководитель – дтн., проф., В.В. Козловский

УДК 428.303

Р.Я. Куций

Національний авіаційний університет
Roman.kucyi@mail.ru

ОСОБЛИВОСТІ ПОШИРЕННЯ РАДІОХВИЛЬ В ЕКРАННИХ ПРИМІЩЕННЯХ

У процесі поширення хвилі піддаються ослаблення і спотворення. Крім того, на приймальну антену впливають різного роду перешкоди як природного, так і штучного походження. Для забезпечення надійної передачі інформації необхідно, щоб поле сигналу, по-перше, в певне число разів перевищувало рівень перешкод (залежно від умов роботи каналу зв'язку і вимог до надійності). По-друге, сигнали не повинні піддаватися надмірним спотворенням, неминуче виникають у процесі розповсюдження. Спотворення повинні знаходитися в межах допустимих норм.

Передача інформації може порушитися або при значному зниженні рівня сигналу (який при цьому вже не буде виділятися на тлі перешкод), або при сильному спотворенні форми сигналу (його розтяганні, дробленні і т. д.).

Вільно поширюються радіохвилі знаходять в сучасній техніці обширні і різноманітні застосування, а саме: в системах зв'язку, в радіолокацій, телеметрії, системах управління, в радіонавігації і в багатьох інших випадках. Їх основна перевага полягає в тому, що коли зв'язок встановлюється між фіксованими (наземними) пунктами, то немає необхідності споруджувати між ними, сполучну або направляючу систему. Радіохвилі є єдиним і природним засобом здійснення зв'язку з об'єктами, що пересуваються (автомобілями, кораблями, літаками, космічними кораблями).

Для радіозв'язку використовуються наступні 12 діапазонів радіохвиль, межі яких по частоті визначаються співвідношенням 0,3 · 10 N -3 · 10 N (тут N - номер діапазону): четвертий - Міріаметровиє хвилі (100-10 км), п'ятий - кілометрові хвилі 10 - 1 км), шостий - гектометрові хвилі (1000-100 м), сьомий-декаметрових хвиль (100-10 м), восьмий - метрові хвилі (10-1 м), дев'ятий - дециметрові хвилі (1,0-0,1 м), десятий - сантиметрові хвилі (10-1 см), одинадцятий - міліметрові хвилі (10 - 1 мм), дванадцятий - децимініметрові хвилі (1,0-0,1 мм).

У системах оптичної і лазерної зв'язку застосовуються частоти чотирнадцятого і п'ятнадцятого діапазонів (до 10 15 Гц).

Діапазон міріаметрових хвиль (3 - 30 кГц) використовується, як правило, для радіозв'язку під водою, діапазони кілометрових (30-300 кГц) і Гектометровиє (300 - 3000 кГц) хвиль застосовуються у звуковому радіомовлення та міжнародної рятувальній службі. На декаметрових хвилях (короткохвильовий діапазон 3-30 МГц) працюють системи далекого звукового радіомовлення, далекого радіотелефонного і телеграфногорадіозв'язку.

Сучасні системи радіозв'язку, призначені для передачі багатоканальних телефонних повідомлень, телебачення, передачі даних зі швидкостями до десятків мегабіт в секунду, працюють в метровому (30-300 МГц), дециметровому (300-3000 МГц) і сантиметровому(3-30ГГц) діапазонах хвиль .

Загальний висновок полягає в тому, що надійність роботи радіоелектронної системи, складовою частиною якої є тракт розповсюдження радіохвиль, повною мірою визначається також надійністю проходження хвиль по тракту. Саме в цьому і полягає роль процесів розповсюдження у сучасній радіоелектроніці.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 654.915

О.О. Корж

Національний авіаційний університет
korzhalexiids@gmail.com

ЗАСТОСУВАННЯ ТЕХНІЧНИХ ЗАСОБІВ СПОСТЕРЕЖЕННЯ ДЛЯ КОНТРОЛЮ ТЕРИТОРІЇ

Будь-який засіб охоронної сигналізації у відповідь на зовнішній вплив, характерне для порушника, що знаходиться в охоронній зоні, виробляє сигнал тривоги з певною ймовірністю. Існує і можливість помилкової подачі тривоги - Р помилкової тривоги. Це викликає необхідність наявності засоби ідентифікації оператором процесів, що відбуваються в охоронюваних зонах і на підступах до них. В якості таких засобів найбільш оптимально з позицій сприйняття людиною-оператором застосування телевізійної апаратури замкнутих відеосистем.

Телевізійні камери і пристрої для їх оснащення

Телевізійні камери. Телевізійна камера - це пристрій, який перетворює оптичне зображення об'єкта, що спостерігається в електричний відеосигнал певного стандарту. Телекамера є найважливішим елементом системи, оскільки

саме з неї в систему надходить первинна інформація про об'єкт і саме її характеристиками визначається якість зображення в цілому.

Камери розрізняють:

- корпусні та безкорпусні;
- чорно-білого і кольорового зображення;
- звичайної і підвищеної чутливості;
- звичайного і високого дозволу;
- для внутрішнього і зовнішнього спостереження;
- для прихованого спостереження.

Пристрої передачі, комутації та обробки відеосигналів

Пристрої обробки і комутації відеосигналів, відеомонітори - це пристрої, що перетворюють відеосигнали в двомірне зображення. Відеомонітори є виробами, спеціально призначеними для використання в ТСВ, тому заміна їх звичайними приймачами телевізійного зображення неприпустима. Крім того, багато відеомонітори забезпечені вбудованими пристроями для прийому сигналів від декількох камер - відеокомутатора. Монітори діляться на два класи - моніторичорно-білого і кольорового зображення.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.735

В.В. Доставалов

Національний авіаційний університет
AceFire-fist@mail.ru

РАСПОСТРАНЕНИЕ ИНФОРМАЦИИ С ПОМОЩЬЮ СИСТЕМЫ WIMAX

WiMAX - это телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов).

Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX следует считать жаргонным названием, так как это не технология, а название форума, на котором Wireless MAN и был согласован).

Технология WiMAX позволяет работать в любых условиях, в том числе в условиях плотной городской застройки, обеспечивая высокое качество связи и скорость передачи данных. WiMAX можно использовать для создания широкополосных соединений "последней мили", развертывания точек беспроводного доступа, организации сети между филиалами компаний и решения других задач, которые ранее были ограничены традиционными технологиями.

WiMAX технология позволяет обеспечить доступ в интернет со скоростями и зоной покрытия, существенно большими, чем у современных сетей WiFi. Wi-Fi – это технология беспроводной связи для небольших расстояний: в офисном здании, кафе и т.п. Расстояние от хот-спота Wi-Fi до компьютера не превышает десятков

метров. Технология WiMax – это сеть широкополосного беспроводного доступа, которая создается на территории целого города, а расстояние от приемника до базовой станции измеряется километрами. В свою очередь, локальные сети Wi-Fi становятся логичным продолжением сетей WiMAX.

Научный руководитель – дтн., проф., В.В. Козловский

УДК 004.056.53

Г.М. Бордюг

Національний авіаційний університет
georgebordiuh@gmail.com

ЗАХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СЕРВЕРНИХ ПРИМІЩЕНЬ

На сьогоднішній день актуальним є питання забезпечення захисту серверних приміщень, так як вони містять важливу інформацію, і її втрата цієї інформації може понести за собою великі втрати.

Безпека серверної кімнати починається з контролю доступу до неї. Картки доступу , біометричні і навіть звукові методи - це загальноприйняті методи,які використовують для обмеження доступу, однак ці методи є первинними і не можуть стовідсотково гарантувати безпеку. Картки , паролі можуть потрапити не в ті руки , а біометричні пристрої досить дорогі і можуть помилково не спрацьовувати на доступ в серверну навіть для тих осіб, яким він дозволений .

Ці заходи можна значно підсилити: наприклад , встановити камери відеоспостереження, фізичну охорону або контактні сенсори . За допомогою комбінування різних методів можна досягнути максимізацію безпеки.

З моменту планування фізична інфраструктура об'єкта повинна сприяти безпеці всього комплексу. Непогано, якщо матеріал стін, стель і підлоги добре захищає приміщення . Якщо вікна чи двері не дозволяють гарантувати безпеку від крадіжок або диверсії конкурентів, потрібно терміново вирішити цю проблему.

На додаток до заходів щодо забезпечення безпеки внутрішньої мережі , необхідно забезпечити фізичний захист і захист мережевого устаткування. Навіть всередині серверної кімнати безпека серверної стійки і встановленого в юнітах обладнання повинна бути максимально можливою. Замки на стійці обмежать доступ сторонніх осіб, захистять від навмисних або випадкових дотиків.

Кожен об'єкт характеризується своїми власними вимогами щодо безпеки . Розробляючи план безпеки для свого серверного приміщення потрібно уважно оцінити всі ризики. Потрібно знайти прийнятний компроміс між безпекою та її вартістю . Комбінуючи можливі ризики з аналізом доступних технологій і вимогам до доступу , цілком реально знайти прийнятне , ефективне рішення.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.056.53

Г.С.Левінсон

Національний авіаційний університет
a.levinson.b@gmail.com

ОСОБЛИВОСТІ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ПІДПРИЄМСТВ

Сотні камер, встановлені на промисловому підприємстві, вимагають серйозного підходу до створення системи відеоспостереження.

Насамперед важливо визначити структуру передачі даних і підібрати обладнання системи, в якому необхідно передбачити всі потреби підприємства та урахуванням специфіки його діяльності. Відеосистема для підприємства повинна забезпечувати відеоконтроль всіх процесів, що відбуваються на підприємстві. Функціонально система повинна забезпечувати взаємодію всіх служб підприємства, яким необхідна відеоінформація.

Необхідно розподілити відеокамери на групи за призначенням і вибрати технічні характеристики відеокамер таким чином, щоб вони вирішували необхідні завдання. Крім того, необхідно не забувати про структуру передачі інформації.

Створення структури передачі інформації залежить від типів застосовуваних відеокамер. Але так як на великих підприємствах доцільно застосовувати різні типи відеокамер, то і середа передачі відеоінформації може бути різною. Практично всі підприємства мають свою локальну мережу, засновану на передачі даних по оптоволоконної лінії зв'язку. І здається, що може бути простіше, ніж просто підключити необхідну кількість камер до внутрішньої мережі підприємства, і система безпеки готова. На жаль, таке рішення має безліч мінусів і не є оптимальним.

Систему відеоспостереження для підприємства необхідно створювати з урахуванням безлічі факторів. Система повинна бути гнучкою, надійною і довговічною. Структура передачі даних повинна бути розрахована на десятки років роботи системи з урахуванням розвитку і розширення. Тому не можна застосовувати побутове та низькоякісне обладнання для системи відеоспостереження на підприємствах. Всі елементи системи повинні мати промисловий стандарт.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.056.53

С.О. Лозицький

Національний авіаційний університет
lozik24@mail.ru

ВИКОРИСТАННЯ СТАНЦІЙ АКТИВНИХ ПЕРЕШКОД

На сьогоднішній день актуальним є питання у використанні станцій активних перешкод у приміщеннях, для запобігання втрат інформації за допомогою несанкціонованого доступу.

Безпека приміщення починається з контролю доступу до неї, але у сучасному світі не обов'язково потрібно бути присутнім у приміщенні для того, щоб незаконно слухати розмову і використовувати отриману інформацію у певних цілях. Мобільні телефони, диктофони, радіожучки замасковані під будь-яку річ – це все предмети, які можуть бути використані для отримання інформації і подальшого її розповсюдження.

Станція активних перешкод, також відома як Глушник – це пристрій який використовується для створення радіоперешкод, що унеможливлює роботу будь-яких приладів радіозв'язку.

Даний пристрій посилає радіохвилі на частоті якій працюють прилади, чим перебиває зв'язок з приймачем і унеможливлює провести зйом інформації за допомогою радіотехніки. Слід відмітити те що різні прибори працюють на різних частотах, тому слід чітко знати, який саме пристрій хочете заглушити, якщо це мобільний телефон то 900/1800МГц, якщо Bluetooth чи Wi-Fi, то 2,4ГГц, якщо частота глушника і приладу не співпадуть, то нічого не вийде і відповідно запобігти втраті інформації через цей канал не вийде. Ще слід знати що станції активних перешкод всенаправлені, тобто випромінюють сигнал у всіх напрямках саме це дозволяє створити поле у якому не буде працювати жоден предмет, який працює на такій же частоті, що і глушник. Потрібно також зважати на те, що радіус дії станції може змінюватися в залежності від багатьох умов таких як: погодні умови, приміщення тощо, і він не буде збігатися з радіусом у паспорті прилада.

Звісно існує ще безліч способів незаконного отримання інформації, але використовуючи станцію активних перешкод, у комплексі з іншими приладами для забезпечення секретності інформації, можна створити досить захищене приміщення.

Ще однією перевагою є те, що у багатьох країнах використання станцій активних перешкод законодавчо незаборонене, а отже, для її встановлення не потрібно оформлювати спеціальні дозволи, що значно спрощує їх використання.

Доступна ціна, відносна простота у використанні, обслуговуванні - робить станції активних перешкод одним із найпопулярніших приладів у боротьбі з несанкціонованим доступом до інформації.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.056.55

Р.М. Бевз

Національний авіаційний університет
headbevz@gmail.com

ЗАХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНОГО ЗВ'ЯЗКУ

На сьогоднішній день актуальним є питання забезпечення захисту мобільного зв'язку, так як людина має право на конфідеційність, і встручання зовнішніми чинниками в її життя є незаконним та неправильним.

Оператори мобільного зв'язку самі забезпечують захист своїх радіоканалів, використовуючи методи шифрування сигналу. При шифруванні використовуються дуже складні алгоритми. Яким саме криптоалгоритмом буде здійснюватися шифрування вибирається на етапі, коли встановлюється з'єднання між базовою станцією і самим абонентом. Ступінь імовірності виникнення витоку інформації про абонента з обладнання оператора, як запевнив оператор, дорівнює практично нулю. Проте, є два методи прослушки абонентів - це активний метод, і пасивний метод.

При пасивному прослуховуванні абонента потрібно використовувати дуже дороге устаткування і мати спеціально навчених працівників.

Другим способом прослушки є активне втручання прямо в ефірі на процес аутентифікації і протоколи управління. Для цього використовуються спеціальні мобільні комплекси. Такі мобільні системи, які, по суті, є парою спеціально модифікованих телефонів і ноутбук.

Визначити що телефон абонента прослуховується саме в цей момент - неможливо, проте, існують додатки для захисту вашого мобільного від прослушки. Ці програми запобігають будь які підключення до помилкових базових станцій. Для визначення достовірності станції використовується перевірка сигнатур і ідентифікаторів станції.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.056.53

О.Г.Роздайбіда

Національний авіаційний університет
bagabondo@mail.ru

ЗАХИСТ В МЕРЕЖАХ Wi-Fi

На сьогоднішній день актуальним є питання забезпечення захисту даних в мережах Wi-Fi. Це пов'язано з стрімким розвитком цих технологій. У наш час практично у кожного з собою є смартфон чи планшет, практично в кожному офісі є велика кількість ноутбуків і всі вони підключені до інтернету. Як зробити це найпростіше? Звісно через бездротову систему Wi-Fi. З цього випливає що використовують її дуже часто, а де велика кількість користувачів, там велика

кількість інформації, яка може бути як не важлива, так і надто цінна для когось. Тому дуже часто такі мережі намагаються зламати, адже стандарт Wi-Fi розроблений на основі IEEE 802.11.

З точки зору безпеки, слід враховувати середовище передачі сигналу, в бездротових мережах отримати доступ до переданої інформації набагато простіше, ніж у провідних мережах. Досить помістити антену в зоні дії. У зв'язку з цим розробляється велика кількість методів захисту цих мереж.

Захист може здійснюватися різними шляхами. Наприклад шляхом обмеження доступу чи автентифікації.

Багато чого залежить від самої організації мережі, наприклад, якщо це Hot-spot мережа, то в ній присутня точка доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але і доступ до зовнішніх мереж. Hot-spot представляє найбільший інтерес з точки зору захисту інформації, бо зламавши точку доступу, зловмисник може отримати інформацію не тільки зі станцій, розміщених в даній бездротовій мережі.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.422

М.В. Михайловський
Національний авіаційний університет
nihto111@gmail.com

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АГРАРНОГО ПІДПРИЄМСТВА

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.).

Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Інформаційна безпека для підприємства полягає у певних діях щодо вияву, усунення та нейтралізації негативних джерел, причин і умов впливу на інформацію.

При цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб'єкта, в умовах якого можлива дія загроз. Досягається це системою заходів, спрямованих на попередження, вияв та ліквідацію цих загроз. Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника.

Головними етапами побудови політики інформаційної безпеки є:

- реєстрація всіх ресурсів, які мають бути захищені;
- аналіз та створення переліку можливих загроз для кожного ресурсу;
- оцінка ймовірності появи кожної загрози;
- вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему.

Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди інтересам підприємства і становлять загрози та ризики для безпеки. Інформаційна безпека в сучасному суспільстві є однією з необхідних умов нормального функціонування підприємства.

Науковий керівник – к.т.н., доц., А.О. Краснопольський

УДК 004.056.53

О.О. Бянкін

Національний авіаційний університет
alexanderbiankin@gmail.com

РАДІОПРОТИДІЯ У СИСТЕМАХ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

З розвитком технологій розвиваються методи перехоплення інформації, виникає необхідність протидіяти гіпотетичному супротивнику, перешкоджаючи перехопленню секретної інформації методами радіопротидії

Основний принцип радіоелектронної протидії – створення перешкод для приймального пристрою з інтенсивністю, достатньою для порушення його роботи.Якщо наперед невідома його робоча частота, то необхідно створитиперешкоду по всьому можливому або доступному діапазону спектру.Достатньо універсальною перешкодою для зв'язних радіоліній вважаєтьсяшумовий сигнал. У зв'язку з цим апаратура радіопротидії повинна включатив свій склад генератор шуму достатньої потужності (на необхіднийдіапазон) і антенну систему. Практично при відношенні верхньої і нижньоїчастоти діапазону більш 2х використовують декілька шумових генераторів і комбінована багатодіапазонна антена.Генератори шуму в мовному діапазоні використовуються для захисту віднесанкціонованого знімання акустичної інформації шляхом маскуваннябезпосередньо корисного звукового сигналу. Маскування проводиться «білимшумом» з коректованою спектральною характеристикою.В деяких випадках наявність декількох випромінювачів необов'язково. Тодівикористовуються компактні генератори з вбудованою акустичною системою,акустичний генератор білого шуму.Головний недолік застосування джерел шумів в акустичному діапазоні – ценеможливість комфортного проведення переговорів. Практика показує, що вприміщенні де «реве» генератор шуму неможливо знаходитися більше 10…15 хв. Крім того, співбесідники автоматично починають намагатисяперекричати засіб захисту, знижуючи ефективність його застосування. Томуподібні системи застосовуються для додаткового захисту дверних отворів,міжрамного простору вікон, систем

вентиляції і т.д.Пристрої віброакустичного захисту використовуються для захиступриміщень, призначених для проведення конфіденційних заходів, відзнімання інформації через шибки, стіни, системи вентиляції, трубиопалювання, двері і т.д. Дана апаратура дозволяє запобігти можливомупрослуховуванню за допомогою дротяних мікрофонів, звукозаписноїапаратури, радіомікрофонів і електронних стетоскопів, лазерного зніманняакустичної інформації з вікон і т.д. Такими здавалося б елементарними засобами можна значно знизити ймовірність несанкціонованого доступу до інформації.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.056.53

Т.С. Запорожець

Національний технічний університет України
«Київський політехнічний інститут»
championka000@gmail.com

ФУНКЦІОНАЛЬНА МОДЕЛЬ БАЗИ ДАНИХ ЗАГРОЗ БЕЗПЕЦІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Державні інформаційні ресурси являють собою певну цінність, мають відповідне матеріальне вираження та вимагають захисту від різноманітних за своєю сутністю впливів. Впливи, які призводять до зниження їх цінності називаються несприятливими та тлумачаться як загрози. Тому для унеможливлення реалізації загроз розробляється та впроваджується комплексна система захисту інформації. Побудова такої системи передбачає визначення потенційних загроз та їх представлення відповідною моделлю. Для формування такої моделі пропонується розробити базу даних загроз безпеці державних інформаційних ресурсів.

Проектування означеної бази даних здійснюється на трьох рівнях: концептуальному, логічному та фізичному. Зокрема, на концептуальному рівні визначається, наприклад, мета побудови бази даних, основні функції, форми представлення даних і вимоги користувачів. Виконання цього переліку завдань здійснено шляхом функціонального моделювання бази даних загроз безпеці державних інформаційних ресурсів в нотації IDEF0. Такий підхід дозволяє здійснити її графічне описання, сформулювати мету та точку зору побудови. Графічний опис відображає базу даних через функцію або набір функцій, що визначають її можливості. Тоді як метою та точкою зору побуди бази даних встановлюється призначення та для кого вона створюється.

Функціональна модель бази даних загроз безпеці державних інформаційних ресурсів в графічній нотації IDEF0 представляється контекстною діаграмою як поєднання відповідних блоків та стрілок зі сформульованими метою та точкою зору. Блок контекстної діаграми є основним її компонентом та моделює означену базу даних. Стрілками позначаються дані або матеріальні об’єкти, що необхідні для формулювання моделі загроз. Так, на вхід блоку подаються реєстраційні дані,

дані авторизації та інформація, що вноситься до бази даних. На виході блоку отримуємо модель загроз безпеці державних інформаційних ресурсів з урахуванням позначених стрілками вимог (обмежень) та ресурсів.

Таким чином, за результатами функціонального моделювання формалізовано використання бази даних загроз безпеці державних інформаційних ресурсів. Зокрема, визначено її призначення, мету та точку зору використання, а також можливості шляхом побудови функціональної моделі.

Означену модель буде використано для створення логічної та фізичної моделей на етапі даталогічного проектування бази даних загроз безпеці державних інформаційних ресурсів.

Науковий керівник – к.т.н., В.В. Цуркан

УДК 004.056

О.В. Швець

Національний авіаційний університет
exundera@yandex.ru

ВИКОРИСТАННЯ АУТЕНТИФІКАЦІЇ ТА КОНТРОЛЮ ДОСТУПУ В СИСТЕМАХ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

З метою забезпечення можливості розмежування доступу до ресурсів АС і можливості реєстрації подій такого доступу кожен суб'єкт (співробітник, користувач, процес) і об'єкт (ресурс) захищається автоматизованої системи повинен бути однозначно ідентифікуємо. Для цього в системі повинні зберігатися спеціальні ознаки кожного суб'єкта й об'єкта, за якими їх можна було б однозначно пізнати.

Ідентифікація - це, з одного боку, присвоєння індивідуальних імен, номерів (ідентифікаторів) суб'єктам і об'єктам системи, а, з іншого боку, - це їх розпізнавання (упізнання) по присвоєним їм унікальним ідентифікаторів. Наявність ідентифікатора дозволяє спростити процедуру виділення конкретного суб'єкта (певний об'єкт) з безлічі однотипних суб'єктів (об'єктів). Найчастіше в якості ідентифікаторів застосовуються номера або умовні позначення у вигляді набору символів.

Таблиця. Порівняння методів аутентифікації.

Параметр	Характеристика абонента				
	Магнітна картка	Відбиток пальців	Відбиток долоні	Голос	Підпис
Зручність у використанні	Добре	Середнє	Середнє	Відмінна	Добре

Ідентифікація порушення	Середнє	Відмінна	Добре	Добре	Відмінна
Ідентифікація законності абонента	Добре	Середнє	Відмінна	Відмінна	Добре
Вартість одного приладу дол..	100	9000	3000	5000	1000
Час розпізнання, с.	5	10	5	20	5
Надійність	Добре	Середнє	Відмінна	Добре	Добре

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 004.056.53

И.А. Вознесенский
Национальный авиационный университет
boton41k_kk@mail.ru

АНАЛИЗАТОР РЕЧИ В СИСТЕМАХ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Распознавание речи – это многоуровневая задача распознавания образов, в которой акустические сигналы анализируются и структурируются в иерархию структурных элементов (например, фонем), слов, фраз и предложений. Каждый уровень иерархии может предусматривать некоторые временные константы, например, возможные последовательности слов или известные виды произношения, которые позволяют уменьшить количество ошибок распознавания на более низком уровне.

На сегодняшний день, под понятием “распознавание речи” скрывается целая сфера научной и инженерной деятельности. В общем, каждая задача распознавания речи сводится к тому, чтобы выделить, классифицировать и соответствующим образом отреагировать на человеческую речь из входного звукового потока. Это может быть и выполнение определенного действия на команду человека, и выделение определенного слова-маркера из большого массива телефонных переговоров, и системы для голосового ввода текста.

Когда заходит разговор о распознавании речи, невозможно оставаться исключительно в сфере «анализа сигналов» (на то есть отдельные труды и отрасли науки). Всегда надо помнить, что при анализе речи мы работаем с особым видом сигнала, который воспроизводится определенной биологической системой. С одной стороны, она ограничена своими амплитудно-частотными характеристиками (АЧХ), а с другой стороны, самим языком и стандартным

набором звуков, которые могут быть произнесены его носителем (например, при анализе русского языка мы не будем принимать во внимание возможность цоканья и свиста). Исходя из поставленной задачи, можно достаточно точно определить характеристики сигнала речи, и его основные свойства.

Научный руководитель – дтн., проф., В.В. Козловский

УДК 004.056.53

О.М. Мельник

Національний авіаційний університет
melnyk.best@gmail.com

РАДІОЛОКАЦІЙНІ ПЕРЕШКОДИ В СИСТЕМАХ ТЗІ

В даний час існує безліч пристроїв радіолокації, радіонавігації та пеленгації. Ними оснащуються сучасні морські судна, літальні апарати, космічні апарати і т. д., причому як цивільні, так і військові. Перешкодою для роботи такого пристрою може стати радіолокаційна перешкода.

Радіолокаційні перешкоди (точніший термін – протирадіолокаційні перешкоди) - це навмисні перешкоди, що ускладнюють або порушують у військових цілях нормальну роботу радіолокаційних (РЛ) коштів: радіолокаційних станцій (РЛС), головок самонаведення керованих ракет або авіабомб, радіовзривателей і т.д.

Розрізняють активні і пасивні радіоперешкоди. Активні перешкоди створюються спеціальними приймально-передавальними або радіопристроїв - станціями або передавачами радіоперешкод, пасивні перешкоди - різними штучними відбивачами радіохвиль. (До пасивних перешкод відносять також відображення радіохвиль від місцевих предметів та природних утворень, які заважають роботі РЛС; ці перешкоди не мають безпосереднього відношення до навмисного радіопротидії). За характером впливу активні радіоперешкоди ділять на маскуючі і імітують (дезорієнтують). Маскуючі перешкоди створюються хаотичними, шумовими сигналами, серед яких важко виділити сигнали, отримані від об'єктів; імітують - сигналами, схожими на сигнали від об'єктів, але містять неправдиву інформацію. Активні маскуючі перешкоди часто мають вигляд радіочастотних коливань, модульованих шумами, або шумових коливань, подібних власних шумах РЛ приймача. Залежно від ширини частотного спектру їх підрозділяють на прицільні, що мають ширину спектра, порівнянну з смугою пропускання РЛ приймача, і загороджувальні, «перекривають» певну ділянку радіочастотного діапазону. Активні перешкоди можуть також мативигляд зондирующих РЛ сигналів, модульованих по амплітуді, частоті, фазі, часу затримки або поляризації (їх формують з зондирующих сигналів, що приймаються на станції перешкод). Такі перешкоди називаються відповідними, вони можуть бути як імітують, так і маскують.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 534.2:004.03

Г.В. Кірієнко

Національний авіаційний Університет
Naterius@ukr.net

ЛАБОРАТОРНІ РОБОТИ З КУРСУ “АКУСТИЧНІ ПОЛЯ І ХВИЛІ”

З давніх-давен одним із головних шляхів передачі інформації була мова, тобто генерування людським організмом певних акустичних коливань. І навіть в час великого прогресу інформаційного та телекомунікаційного прогресу мова займає досить важливе місце в поширенні інформації. Акустичний канал витку інформації займає велику роль в ТЗІ. В нашій країні досить погано дотримується системи контролю норм будівництва та акустичної ізоляції приміщень, в деяких окремих випадках перебиваючи па першому поверсі можна почути про що йде мова на третьому. Тож для захисту інформації від витку акустичним каналом потрібно розуміти як поширюються акустичні коливання і як воші можуть бути знятті злочинцем.

Тож в зв’язку з цим доцільно розробити та впровадити курс лабораторних робіт з «Акустичні поля і хвилі».

Сутність даного курсу полягає в тому щоб майбутній спеціаліст набув не тільки теоретичних, а і практичних навичок в вивченні акустичного каналу витоку інформації. Набув практичних вміння для визначення таких каналів як акустичний, вібро-акустичний та акусто-електричних каналів витоку інформації, здобув навички по нейтралізації таких каналів витоку інформації. Створити та проаналізувати модель загрози для акустичного каналу, промоделювати та розробити ефективний план по нейтралізації можливих загроз для акустичного каналу тощо. В курс лабораторних робіт також входить, моделювання поширення акустичних хвиль, можливість використання акустичних хвиль, для захисту інформації.

Конструкція, яка буде використовуватися в лабораторних роботах дасть змогу отримати обширне знання про природу акустичних коливання, вплив актустичних коливань, на різного роду матеріалів. Розповсюдження та траєкторію руху коливань.

Після проходження такого комплексу лабораторних робіт студент самостійно зможе визначати акустичні канали витоку інформації та закривати ці канали за допомогою набутих знань.

Науковий керівник – к.т.н., доц., В.О. Темніков

УДК 681.3

І.В. Лавренчук

Національний авіаційний університет
lavrenchyk.igor@gmail.com

ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Одним із найпоширеніших підходів до оцінки якості захисту інформації є визначений поділ реалізованих функцій і завдань, експлуатаційних характеристик і вимог у відповідність технічним завданням на створення системи захисту. Інший спосіб, який використовується у вітчизняній та закордонній практиці – це аналіз функціональної надійності системи, яка також характеризує якісний рівень системи інформаційної безпеки (СІБ).

Існують наступні методи та засоби оцінки ефективності СЗІ:

1. Метод порівняльного багатовимірного аналізу. Цей метод створений для визначення ступеня взаємного впливу загроз та причин їх виникнення. Суть методу можна звести до такого узагальненого алгоритму:

– складається перелік об'єктів, що оцінюються, і вибираються ознаки, за якими буде проводитись оцінка. В даному випадку під об'єктами оцінки будемо розуміти показники захищеності обчислювальної системи, а під ознаками – сукупність параметрів, що характеризують ці показники;

– цей перелік слугує основою для формування матриці ознак X(n,w), де n – кількість ознак, а w – кількість об'єктів, що оцінюються. Кожному об'єкту ставиться у відповідність рядок матриці із n ознак;

– через те, що дані, які зведені в матрицю, описують різні властивості об'єктів і мають різні одиниці виміру, вихідна матриця нормалізується відповідно до формули

$$Z_{ik} = \frac{x_{ik} - \overline{x_k}}{S_k}$$

де

$$\overline{x_k} = \frac{1}{w}\sum_{i-1}^{w} x_{ik}$$

– середнє арифметичне ознаки k по усіх об'єктах,

$$S_k = \left[\frac{1}{w}\sum_{i-1}^{w}(x_{ik} - \overline{x_k})^2\right]^{\frac{1}{2}}$$

– стандартне відхилення ознаки k

Z_{ik} – нормалізоване значення ознаки k для одиниці об'єкта i ;

– проводиться розрахунок елементів матриці від- станей між показниками захищеності з урахуванням усіх елементів матриці ознак

$$W_{rs} = \frac{1}{n}\sum_{k-1}^{n}|z_{rk} - z_{sk}| \quad ,(r,s=1,2,3,...,w).$$

2 Методи аналізу ризиків інформаційних систем (ІС). На даний час при побудові СЗІ АС особливого значення набуває завдання побудови моделей загроз інформації. Існує чимало алгоритмів, які здійснюють аналіз ризиків ІС. До найбільш відомих алгоритмів належать CRAMM і RiskWatch. Зазначені алгоритми мають ряд переваг та набули широкого поширення.

Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються один від одного своїми базами знань.

Науковий керівник – доц., В.В. Литвин

УДК 004.032.26

М.П. Мартиненко

Національний авіаційний університет

АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ВІДЕОАНАЛІТИКИ

Відеоаналітика — апаратно-програмне забезпечення або технологія, що використовують методи комп'ютерного зору для автоматизованого збору даних на підставі аналізу потокового відео (відеоаналізу). Відеоаналітика спирається на алгоритми обробки зображення і розпізнавання образів, що дозволяють аналізувати відео без прямої участі людини. Відеоаналітика використовується у складі інтелектуальних систем відеоспостереження (CCTV, охоронного телебачення), управління бізнесом (business intelligence, BI) і відеопошуку.

Залежно від цілей, відеоаналітика може реалізувати як одну, так і декілька базових функцій: виявлення об'єктів, стеження за об’єктами, класифікація об'єктів, ідентифікація об'єктів, виявлення (розпізнавання) ситуації.

З точки зору застосування, розрізняють такі типи відеоаналітікі:

Периметральна відеоаналітіка застосовується для охорони протяжних ділянок і периметрів, виявлення вторгнення і перетину сигнальної лінії в «стерильної зоні».

Ситуаційна відеоаналітіка застосовується для розпізнавання тривожних ситуацій, пов'язаних з поведінкою людей або з рухом транспортних засобів.

Бізнес-аналітика застосовується для управління організацією, оцінки продуктивності персоналу, оптимізації бізнес-процесів і досліджень поведінки клієнтів.

Біометрична відеоаналітіка (biometrical video analytics) застосовується для ідентифікації та супроводу осіб за біометричними ознаками особи

Номерна відеоаналітіка застосовується для розпізнавання реєстраційних знаків автомобілів, а так само для аналізу їх руху за даними безлічі камер.

Багатокамерна відеоаналітіка застосовується для супроводу об'єктів за допомогою безлічі камер.

Технологічна відеоаналітіка застосовується для моніторингу технологічний процесів, забезпечення якості виробництва, підвищення продуктивності.

Головні переваги відеоаналітікі перед звичайними системами відеоспостереження полягає в автоматичному виділенні метаданих з потоку відеоданих без участі оператора. Отримані метадані можуть бути використані для швидкого пошуку в відеоархіву, розсилки тривожних сповіщень та збору статистики. У порівнянні з «ручним відеоспостереженням», відеоаналітіка дозволяє зменшити вартість відеомоніторингу і людського фактора в частині виявлення і часу реагування. Так як значна частина відеоданих (більше 99%) в системах відеоспостереження не представляє інтересу для користувачів, відеоаналітіка дозволяє кардинальним чином зменшити навантаження на канали зв'язку і систему архівування за рахунок фільтрації непотрібних відеоданих.

Головною проблемою багатьох впроваджень відеоаналітікі є висока частота помилкових спрацьовувань, яка швидко зменшує економічний ефект технології. Проблема поступово вирішується шляхом вдосконалення алгоритмів відеоаналізу, автоматичного тестування на спеціальних випробувальних стендах та ранжування подій за важливістю. Інша проблема полягає в істотній вартості системної інтеграції та впровадження відеоаналітікі. Роль цього фактора знижується завдяки появі відкритих стандартів, таких як ONVIF, спрощення процедур калібрування і настройки відеоаналітики.

Науковий керівник – к.т.н., доц., Т.В. Німченко

УДК 004.32.26

В.Д. Кирилюк

Національний авіаційний університет
vovan.k.d@gmail.com

ВИЯВЛЕННЯ ЗОНДУВАННЯ АТАКИ З ВИКОРИСТАННЯМ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання отримання узагальненої оцінки рівня захищеності інформації на основі методології, що враховує як кількісні, так і якісні показники оцінки. На сьогоднішній день, практично на будь-якому об'єкті ОІД реалізована комп'ютерна мережа. У зв’язку з швидким поширенням комп'ютерних мереж, з’явилося багато проблем з безпекою.

В останні роки число нападів на мережу різко збільшилося, тому забезпечення безпеки мережних ресурсів є дуже істотним завданням. Ці напади є основами інших атак типу DOS, R2U, U2R та ін. Отже, системи захисту від таких атак - це необхідність. Ці атаки не втягуються в активну діяльність, але в основному знаходяться в пасивному стані, і з'ясовують, які машини активні або перебувають у мережі, які сервіси використовуються користувачем і т. д. Насправді зловмисники або хакери використовують різні зондувальні інструменти, щоб отримати недоліки у системі, різного роду установки або алгоритми, які можуть

допомогти в їх активних атаках. У процесі виявлення вторгнень є дві категорії - зловживання і виявлення аномалій. Категорія зловживання - це загальна категорія виявлення вторгнень, яка працює шляхом визначення видів діяльності, які змінюються в залежності від встановлених закономірностей для користувачів або груп користувачів. Це, як правило, передбачає створення баз знань, у яких міститься характеристика досліджених видів діяльності. Другий метод передбачає порівняння діяльності користувача з відомою поведінкою зловмисників, що намагаються проникнути в систему. Виявлення зловживань також використовує базу знань інформації. В основному, засоби виявлення атак використовують оцінки параметрів, таких як позитивні і хибно-негативні рівні виявлення. Помилкове спрацьовування відбувається, коли система класифікує дії як аномальні (можливого зараження), коли це законні дії. У той час як хибно-негативні виникають, коли фактичні нав'язливі дії мали місце, але система дозволяє їм передати інформацію в якості природньої поведінки.

Основна проблема захисту інформації шляхом створення штучної нейронної мережі є велика кількість хибно-позитивних і хибно-негативних спрацьовувань. Для виявлення кількісних характеристик були почергово введені в мережу різного роду пробники атак.

Результатом є те, що наша система є найбільш ефективною для захисту інформації, та мають майже 100% захищеність та близько до 0% хибно-позитивних і хибно-негативних спрацьовувань.

Науковий керівник – д.т.н., проф., В.В. Козловський

УДК 621.396.962.2(043.2)

А.М. Олійник

Національний авіаційний університет

ВИКОРИСТАННЯ НЕЛІНІЙНОГО ЛОКАТОРА

Нелінійні локатори використовуються в різних сферах для виконання різноманітного завдання . Виконуючи пошук закладних пристроїв або інших технічних засобів нелінійний локатор може виявити пристрій незалежно від того ввімкнутий він чи ні.

Найчастіше при роботі з локатором зустрічаємось з помилковим спрацюванням при пошуку напівпровідника , тому що недалеко знаходяться різні електричні пристрої або спрацювання на металічні предмети в зоні пошуку. Після опромінення предмета або стіни , сигнал відбитий повертається на гармонічних частотах через нелінійні властивості з'єднання . Але можливі помилкові спрацювання , коли поле опромінення попадає з'єднання двох різних металів через окислення , що викликає гармонічні сигнали через нелінійні характеристики .Отримавши відбитий сигнал порівнюємо другу та третю гармоніку , що дає нам змогу отримати інформацію про предмет . Оскільки нелінійний локатор має завдання по пошуку закладних пристроїв , тобто пошуку напівпровідникових переходів , порівнюємо другу та третю гармоніку . При наявності н/в отримаємо

високий рівень другої гармоніки та низький третьої . Використання ефекту затухання в поєднанні з роботою в безперервному режимі досягає досягти кращих властивостей для пошуку пристроїв які закладені в місцях де не можливо оцінити предмет без відповідних дій .Використовуючи антену ФАР , отримаємо діаграму направленості , що дозволяє знайти майже точне місце розташування пристрою

Таким чином , нелінійний локатор – складний пристрій , що дозволяє виконати роботу по пошуку закладних пристроїв які приховані , не затрачаючи багато часу.

Науковий керівник – к.т.н., доц., С.М. Скворцов

УДК 621.396.962.2(043.2)

О.І. Оселедько

Національний авіаційний університет

ЗАСТОСУВАННЯ ФАР В РОБОТІ НЕЛІНІЙНОГО ЛОКАТОРА

Завданням нелінійного локатора є виявлення і визначення місця розташування прихованих електронних засобів промислового шпигунства, як випромінюючих, так і не випромінюючих.

Важливою перевагою АФАР є можливість реалізувати діаграму спрямованості веєрного типу з шириною основного пелюстка в межах ± 45° в одній площині і 1,5° – 2° в перпендикулярній. Її точний напрям і орієнтацію на об'єкті сканування вказує, закріплений на локаторі, лазер. Іншим лазером, закріпленим на штативі, фіксується положення діаграми спрямованості в момент виявлення нелінійних елементів. Для визначення точного місця розташування сканування проводять ще раз з поворотом площини діаграми спрямованості на 40° - 60°.

Фіксована фаза випромінюючих елементів реалізується мікрополосковими фазообертачами. Відсутність потреби в переналаштуванні фаз і відсутність механічних фазообертачів зменшує масо-габаритні характеристики локатора і споживання електроенергії.

Для частотної селекції використовуються фільтри, що в СВЧ діапазоні представляють собою лінію передачі, включаючи неоднорідності узгоджені в визначеній полосі пропускання і різко неузгоджені за її межами.

Локатор неперервного випромінювання дозволяє реалізувати сканування на менші відстані ніж імпульсний, але при роботі в будівлях, через насиченість об'єктів обстеження і сусідніх приміщень електоронною технікою і контактними завадними об'єктами, реальна дальність дії встановлюється оператором на рівні 1-0,5 м, шляхом зниження потужності випромінювання, що дозволяє визначити, від якого саме об'єкта прийшов відгук.

Неперервний режим роботи дозволяє випромінювати ту ж енергію при меншій потужності, тому не створює проблем по частині електромагнітної сумісності та екологічно нешкідливий.

Частота випромінювання 900 МГц, оскільки довжина хвилі опромінюючого електромагнітного поля повинна бути відносно рівною за величиною з розмірами

об'єктів пошуку. На більш довгих хвилях інтенсивність відбитого поля буде мізерна через явища дифракції, огинання поля навколо об'єкта. На більш коротких хвилях - нелінійні властивості об'єктів пошуку різко падають, через явища затухання.

Науковий керівник – к.т.н., доц., С.М. Скворцов

УДК 004.056(043.2)

А. В. Швец

Национальный авиационный университет
exundera@yandex.ru

ЭКСПЕРИМЕНТАЛЬНАЯ СИСТЕМА ДЛЯ АДАПТИВНОГО ПОДАВЛЕНИЯ АКУСТИЧЕСКИХ КОЛЕБАНИЙ

В работе предложена адаптивная система, позволяющая организовать защиту информации по акустическому каналу.

Адаптивная система подавления акустических колебаний включает в себя переносной компьютер с рядом специального программного обеспечения: Steinberg WaveLab, Adobe Audition, Cakewalk Sonar, Mathcad и генератор звуковых частот. В данном случае используется несколько программ для аудио редактирования, в связи с тем, что их возможности в обработке сигналов несколько различаются.

Например, в программном пакете Steinberg WaveLab использовались возможности мониторинга, а именно: осциллограф, два анализатора спектра сигнала, панорама фазы и уровня сигнала. Все эти компоненты очень удобно использовать для мониторинга.

Для более качественной обработки звука использовалась программа Adobe Audition. Данное программное обеспечение позволяло проводить углублённое редактирование за счёт набора своих эффектов и возможностей анализаторов спектра сигнала и его фазы. Также была возможность вручную изменять амплитуду практически в любой точке временной шкалы после записи сигналов.

Из программы Cakewalk Sonar были задействованы базы эффектов, которые позволили удобно манипулировать фазой сигнала для компенсирующей акустической системы.

В программе Mathcad была смоделирована математическая модель адаптивного подавления акустических колебаний.

Для экспериментальных исследований использовались внешние чувствительные микрофоны, внешний осциллограф, внешний генератор звуковых частот и акустические системы, позволяющие имитировать плоскую акустическую волну.

Акустические системы (АС) использовались следующим образом - одна АС была источником тональных сигналов, т.е. источником или имитатором речевого информационного сигнала, а другая в том же направлении излучала тот же сигнал, но с фазой перевёрнутой на 180 градусов, т.е. использовалась как подавляющая

адаптивная акустическая система. В результате по направлению распространения волн образовывалась «зона тишины».

Таким образом, разработанная система для адаптивного подавления акустических колебаний, позволила провести исследования по адаптивному подавлению акустических колебаний, что, возможно, в будущем позволит создать адаптивную систему по защите информации от утечки по акустическому каналу.

Научный руководитель – асс., Р. Д. Цигвинцев

ЗБІРНИК ТЕЗ

науково-практичної студентської конференції
«ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

5-6 березня 2015 р.

Київ

Комп'ютерна верстка: Краснопольський А.О.
Адреса для контактів: rit@nau.edu.ua