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

ЗБІРНИК ТЕЗ

науково-практичної студентської конференції
«ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

14-15 березня 2016 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:

(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:

(2)

Тоді коефіцієнт ефективності:

(3)

де Рві – імовірність вірного виявлення і-го сповіщувача;

Сі – ціна і-го сповіщувача;

i = 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 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 621.391.(075.8.)

І.В. Івахіна

Національний авіаційний університет
ii-94@mail.ru

РОЗПІЗНАВАННЯ СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ НЕЙРОПОДІБНИХ СТРУКТУР

Одним з можливих каналів витоку інформації є випромінювання елементів комп'ютера, точніше, елементів основних технічних засобів (ОТЗ), якщо говорити

про захищені автоматизовані системи (АС). Приймаючи і декодуючи ці випромінювання, можна отримати відомості про всю інформації, що обробляється в комп'ютері. Цей канал витоку інформації називається ПЕМВН (побічного електромагнітного випромінювання і наведення). У Європі та Канаді застосовується термін «compromising emanation» - компрометуюче випромінювання. В Америці застосовується термін «TEMPEST».

Частоти, на яких можуть випромінюватися (наводитись) інформативні сигнали, залежать від типів та видів апаратурних засобів, визначається тактовою частотою використовуваного засобу обробки інформації і можуть знаходитись у діапазоні від сотень Гц до кількох десятків ГГц. Складові комп'ютера (монітор, клавіатура, жорсткий диск та ін.) створюють різні рівні ПЕМВН.

Методологія якісного оцінювання рівня захищеності інформації в системі ґрунтується на результатах вимірювань та експертних оцінках, якість яких визначається кваліфікацією та підготовкою експертів, що призводять до низького рівня захищеності інформації. Експертні дані можуть бути нечіткими і недостатньо вираженими для того, щоб бути описаними математичними залежностями. Крім того, така інформація може бути різноякісною, а оцінка значень параметрів проводиться за рахунок різних шкал. Але часто функціонування таких систем можливо описати в вигляді евристичних уподобань, використовуючи конструкції в формі нечітких правил або відношень різного типу.

Авторами запропонована модель нейроподібної системи оцінки рівня захищеності інформації, застосовуючи теорію нечітких продукційних моделей (мереж). Модель системи є універсальною, достатньо ефективною, описується мовою, близькою до природньої.

Пропонується метод розпізнавання реакції на еталонні тестові сигнали, що використовує ортогоналізації й обчислення коефіцієнтів розкладання в базисі, побудованому за асоціацією з вхідними сигналами, що "навчають", систему у відповідності з теорією побудови нейроподібних діагностичних систем. Даний метод є кращим з погляду адаптивних властивостей і зручний в силу свого ітеративного характеру.

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

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 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 004.056.53

А.В. Яковлєв

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

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Бездротові технології все більше поширюються у всі сфери життя. Все це стало можливим завдяки досягненням сучасних цифрових методів модуляції, кодування, пакетної обробки даних. Прогресивним кроком у розвитку бездротового зв'язку було розроблення стандартних міжнародних протоколів передачі даних, що давали можливість об'єднати досвід спеціалістів різних країн і забезпечити сумісність пристроїв різноманітних виробників. Життєздатність бездротових технологій підтверджують успішно використовувані Bluetooth та Wi-Fi.

На сьогоднішній день актуальним є питання забезпечення захисту даних в мережах Wi-Fi. За дуже короткі терміни бездротові технології стали потужним інструментом обміну інформації у багатьох галузях людської діяльності.

Технологія бездротових мереж Wi-Fi є найзручнішою, оскільки забезпечує мобільність, легкість установлення та використання. 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 кількість інформації, яка може бути як не важлива, так і надто цінна для когось. Тому дуже часто такі мережі намагаються зламати, адже стандарт WiFi 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 зі станцій, розміщених в даній бездротовій мережі. Бездротові технології продовжують свій стрімкий розвиток у світі і вже сьогодні вони не відстають від провідних технологій за швидкістю і якістю передачі інформації.

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

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

А.С. Комар

Національний авіаційний університет
komariiik@ukr.net

СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ ІНТЕРНЕТ ПРОВАЙДЕРА

Створення системи захисту інформації для організацій, що займаються наданням телематичних послуг, є обов'язковою складовою діяльності організації

Інтернет-провайдера. Дана необхідність зумовлена тим, що подібні організації обробляють великий обсяг конфіденційних відомостей, у тому числі персональні дані, захист яких обов'язкова за вимогам законодавства. Жорстка конкуренція на ринку призводить до того, що конфіденційна інформація, якою володіє організація, може дати значну конкурентну перевагу. Також комплексна система захисту інформації дозволить забезпечити безперебійне функціонування сервісів, запобігти прямі матеріальні втрати від витоку або втрати конфіденційної інформації, а також запобігти можливому збитку репутації компанії.

Для того, щоб визначити доцільність створення КСЗІ, зону і глибину її охоплення слід провести детальний аналіз організації, що включає:·аналіз діяльності підприємства. Положення організації на ринку. Виявлення конфіденційної інформації та захищаються. Аналіз загроз, вразливостей і потенційного збитку від реалізації загрози.

На основі отриманої інформації про діяльність організації та вразливі місця у діючій системі захисту необхідно скласти технічне завдання на створення комплексної системи захисту інформації.

Та частина ризиків, якої часто приділяється занадто мало уваги. Суть даної групи ризиків полягає в тому, що по-перше поточний стан інформаційної системи організації має задовольняти вимоги впроваджуваних заходів, по-друге впроваджувані технічні заходи повинні перебувати в гармонії з організаційними та програмно-апаратними заходами. Можливі ризики: Конфлікт встановлюваного програмного і апаратного забезпечення зі встановленою операційною системою і апаратною частиною· Складність в експлуатації технічних і програмних засобів· Наявність закладних пристроїв в встановлюваних апаратних засобів· Наявність декларованих можливостей в інсталюються програмних засобахОсновні заходи запобігання даної групи ризиків:· Перевірка всіх поставляються програмних і апаратних засобів· Вибір надійних постачальників. Ретельний вибір необхідних програмних та апаратних засобів.

За допомогою складеної структури організації була розрахована матриця відповідальності, яка дозволяє виявити відповідальних за той чи інший захід. Завдяки детальному плану заходів можна оцінити загальну підсумкову вартість побудови комплексної системи захисту інформації. Незважаючи на досить високу вартість створення комплексної системи захисту інформації, дані заходи повністю окупають себе з причини високої вартості інформації, що захищається.

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

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

ПОРІВНЯННЯ ЧАСУ РОБОТИ АЛГОРИТМІВ ОЦІНКИ ПАРАМЕТРІВ КАНАЛІВ ЗВ'ЯЗКУ IP-МЕРЕЖІ В ЗАДАЧІ ПОБУДОВИ СИСТЕМИ ВІДЕОКОНФЕРЕНЦЗВ'ЯЗКУ

В даний час система багато точкових відеоконференц зв'язків (МВКС) широко використовується при вирішэнні різних завдань. Основою таких систем є ефективна топологія мережі, що дозволяє передавати великі обсяги відео даних з мінімальним навантаженням на мережу. Для побудови такої топології необхідно швидко, точно і з мінімальним використанням службового трафіку визначати характеристики окремих каналів зв'язку в мережі.

Метою роботи є порівняльний аналіз часу роботи алгоритмів за оцінкою доступної смуги пропускання і затримки в каналах зв'язку.

В ході роботи розроблено новий алгоритм, що дозволяє отримувати інформацію про доступну смугу пропускання і затримки в каналах зв'язку. Проведено порівняльний аналіз роботи нового і відомих алгоритмів за допомогою окремої ділянки IP-мережі. У тестуванні враховувалися різні етапи функціонування систем МВКС (первинне встановлення з'єднання і побудова топології мережі, а також етап активного спілкування, коли топологія мережі не змінюється). Для спрощення математичної моделі вважаємо, що величина смуги пропускання кожного з каналів зв'язку не змінюється під час однієї сесії МВКС.

У фазі початкової побудови топології мережі ВКЗ час роботи нового алгоритму зменшилася на 8% і 3% в порівнянні з алгоритмами IGI-PTR і Abing відповідно. При активній фазі спілкування учасників МВКС час вимірювання для всіх алгоритмів відрізнявся незначно (не більше 1%). Даний результат пояснюється тим, що після етапу встановлення з'єднання всі алгоритми вже зійшлися до певних значень доступної смуги пропускання і затримки, а флуктуації відео-трафіку МВКС слабо впливають на різницю часу вимірювання.

Надалі планується порівняти створений алгоритм з такими алгоритмами як Assolo і pathChirp, які відомі своєю високою швидкістю роботи, але мають істотний недолік у вигляді великого об'єму службового трафіка, необхідного для роботи алгоритмів..

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 $0{,}3 \cdot 10^{N-3} \cdot 10^{N}$ (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

ДВОХФАКТОРНА АВТЕНТИФІКАЦІЯ ЯК МЕТОД ДЛЯ НАДІЙНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Коли мова йде про захист інформації, одним з найважливіших аспектів є захист від несанкціонованого доступу до ресурсів нашої мережі. Зрозуміло, вкрай важливим питанням є забезпечення процедури безпечної автентифікації. Цілком очевидно, що будь-яке розмежування повноважень, настройка прав доступу на ресурси системи має сенс тільки в тому випадку, якщо ми впевнені в тому, що той, хто намагається отримати доступ до наших ресурсів, є легальним користувачем.

Двохфакторна автентифікація або 2FA - це метод ідентифікації користувача в будь-якому сервісі, де використовуються два різних типи автентифікаційних даних. Введення додаткового рівня безпеки забезпечує більш ефективний захист акаунта від несанкціонованого доступу.

Двохфакторна автентифікація вимагає, щоб користувач мав два з трьох типів ідентифікаційних даних: щось йому відоме, щось у нього наявне, щось йому притаманне (біометрія). Очевидно, що до першого пункту належать різні паролі, пін-коди, секретні фрази і так далі, тобто щось, що користувач запам'ятовує і вводить в систему при запиті. Другий пункт - це токен, тобто компактний пристрій, який знаходиться у власності користувача. Найпростіші токени не вимагають фізичного підключення до комп'ютера - у них є дисплей, де відображається число, яке користувач вводить в систему для здійснення входу - складніші підключаються до комп'ютерів за допомогою USB і Bluetooth-інтерфейсів. Сьогодні в якості токенів можуть виступати смартфони, тому що вони стали невід'ємною частиною нашого життя. У цьому випадку так званий одноразовий пароль генерується або за допомогою спеціального додатку (наприклад Google Authenticator), або приходить по SMS - це максимально простий і дружній для користувача метод, який деякі експерти оцінюють як менш надійний.

Щоб користувач міг здійснити вхід, між токеном клієнта і сервером автентифікації повинна існувати синхронізація. Головна проблема полягає в тому, що з часом вони здатні розсинхронізуватися, проте деякі системи, такі як SecurID компанії RSA, дають можливість повторно синхронізувати токен з сервером шляхом введення декількох кодів доступу. Більш того, більшість з цих пристроїв не мають змінних батарей, тому мають обмежений термін служби.

Методам захисту, заснованим на методиках багатофакторної автентифікації, сьогодні довіряє велика кількість компаній, серед яких організації зі сфери інформаційних технологій, фінансового і страхового секторів ринку, великі банківські установи та підприємства державного сектору, незалежні експертні організації, а також дослідницькі фірми.

Науковий керівник – доцент, к.т.н., В.А. Швець

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 004.239

С.О. Лозицький

Національний авіаційний університет
lozik24@mail.ru

ЗАХИСТ ІНФОРМАЦІЇ У ЛОКАЛЬНИХ МЕРЕЖАХ

У наші дні інформація є одним із найцінніших і найкоштовніших ресурсів. Оскільки людство дуже швидкими кроками відходить від зберігання паперових, а все більше і більше віддається перевага електронним носіям, які можуть зберігати інформацію десятиліттями. Також із входом у наше життя комп'ютерів життя суттєво полегшало, тепер десь у замкненій кімнаті стоїть сервер на якому зберігається вся інформація і не потрібно нікуди ходити, нічого носити переписувати, усе робиться за допомогою кількох кліків мишкою, або набором кількох команд. Тому зловмисники шукають все нові і нові способи добування інформації, оскільки у багатьох фірмах і установах усі ПК зв'язані у локальну мережу, а та у свою чергу із глобальною мережею Інтернет, то все частіше і частіше саме через них зловмисник і намагається здобути бажані данні. Слід зазначити, що серверна кімната як правило гарно захищена і знаходиться далеко від працівників, то добратися напряму до неї дуже важко, тому саме вхід у мережу віддаленим доступом являється одним із найпопулярніших методів. Існує безліч методів улаштування локальної мережі, на основі різних операційних систем за

допомогою різного обладнання, різних конфігурацій і т.д. Але буває і так, що під час системного збою пропадає інформація. Основною роботою системного адміністратора і є забезпечення безперешкодної роботи навіть у екстремальних ситуаціях.

Слід зазначити що останнім часом все більше і більше набирає обертів будувати мережі на основ POSIX сумісних UNIX системах, оскільки дана система дає найточніше налаштування прав користувачів, а система контролю дає можливість уберегти сервер від небажаної атаки, статистика каже що більшість успішних атак на такі мережі були здійснені саме через те, що адміністратор не зовсім правильно розставив права доступу, що і стало коміркою через яку була поцуплена інформація. Зараз даними системами обладнують термінали, банкомати, програмне ПЗ, саме через широку можливість контролю правами, саме через це данні системи і не підвергаються атакам вірусів, адже файлова система побудована таким чином, що вірус не зможе розповсюджуватися по ній, бо кожен його крок підлягає авторизації і верифікації, що на даний момент неможливо реалізувати програмно.

Зараз мережа являється одним із основним засобів обміну інформацією, а отже її захист дуже важливий, бо втрата інформації може завдати неповторних збитків, а також тягти за собою важку відповідальність.

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

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

АНАЛІЗ ВІБРОАКУСТИЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Захист мовної інформації від можливого витоку по технічних каналах є однією з приорітетних задач забезпечення інформаційної безпеки. Для перехвату мовної інформації використовується велика кількість засобів, які дозволяють знімати інформацію з наступних каналів: акустичних, віброакустичних, акусто-оптичних та інших. Насамперед, основну увагу слід приділяти активним методам захисту інформації до яких належать віброакустичні системи захисту.

Зазвичай системи активного віброакустичного захисту складаються з генератора шуму, акустичних випромінювачів та сукупності вібропереторювачів.

Провівши аналіз генераторів віброакустичних завад можливо виділити проблеми, які виникають підчас їх використання. До них належать: висока споживча потужність, виникнення паразитних акустичних шумів, незадовільні масо-габаритні показники, невисокі ККД. Окрім цього рівень паразитних акустичних перешкод, що створюється системою віброакустичних зашумлень є також важливою характеристикою систем віброакустичного захисту, тому при роботі даної системи постає задача зменшення зазначеного рівня шумів при збережені високої вібровіддачі.

Високі вимоги висуваються також і до джерела електричного сигналу захисного зашумлення, яке використовується в системах віброакустичного захисту інформації.

Так, усі канали кожного з генераторів повинні бути цілком незалежними, тобто до складу кожного каналу повинні входити – вихідний підсилювач, задаючий генератор білого шуму та коректор спектру. Це важливо, як для підвищення надійності пристрою в цілому, так і для покращення якості захисту, адже підвищення ефективності системи віброакустичного захисту потребує вдосконалення технічних рішень стосовно складових частин (вихідних блоків генератора шуму).

Отже, підвищення ефективності систем віброакустичного захисту інформації можливе за рахунок вдосконалення генератора шуму, вихідного підсилювача потужності та засобів корекції.

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

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 004.422

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 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 681.327.12.001.362

А. В. Швец

Национальный авиационный университет
exundera@yandex.ru

АЛГОРИТМ АВТОМАТИЧЕСКОГО ПОИСКА И ЛОКАЛИЗАЦИИ ОБЛАСТИ ЛИЦА НА ИЗОБРАЖЕНИИ

В настоящее время активно развиваются биометрические технологии. Их целью является разработка автоматизированных систем идентификации человека на основе биометрических признаков. Ожидается, что применение подобных систем существенно уменьшит количество преступлений, связанных с несанкционированным доступом. Технология идентификации человека на основе изображений лиц признана наиболее приемлемой для массового применения, так как она не требует физического контакта с устройством, ненавязчива, естественна и, в потенциале, может обладать высокой надёжностью и скоростью.

Именно на этом возможно создать ситему доступа к персональному компьютеру, используя различные видеокамеры.

В такой системе возникает задача автоматизированного выделения лица на общем фоне, поиск характерных фрагментов и идентификация.

Цель работы – разработка алгоритма автоматического поиска и локализации области лица на изображении.

Голова человека представляет собой объект с достаточно устойчивыми внешними признаками (в основном это брови, глаза и нос). Верхняя и нижняя части головы могут существенно отличаться у людей разного возраста, пола, расы в основном за счёт наличия/отсутствия волосяного покрова и, в меньшей степени, из-за особенностей анатомического строения. Следует отметить также, что цвет/оттенок кожи и вариации в освещении могут в той или иной мере «маскировать» лицо, особенно на пестром фоне. Дополнительные затруднения вызывает отсутствие априорной информации, например, о размерах головы на фотопортрете.

Для преодоления указанных сложностей на первом шаге выполняется операция выделения краёв на изображении. Пусть A(x,y) – изображение размером m×n пикселей. Под свёрткой изображения A(x,y) с некоторой маской H(x,y) размером k×l будем подразумевать преобразование A(x,y)→ A’(x,y), при котором каждый элемент изображения A’(x,y) будет получен следующим образом:

$$a_{ij}^{l} = \sum_{i'=1}^{n} \sum_{j'=1}^{m} a_{i-i'j-j'} \times h_{i'j'}$$

Где маска – набор используемых для свёртки весовых коэффициентов, расположенных таким образом, чтобы отражать пространственные отношения между элементами, к которым они применяются.

Из-за специфики задачи, получение надежных результатов, в том числе и на слабоконтрастных изображениях будем применять оператор Собеля.

Оператор представляет собой свертку исходного изображения с двумя масками Sh и Sv размером 3×3 по отдельности и суммирование результатов

В результате, оценив каждую из областей изображения, где может находиться лицо, выбирается та, при сравнении с которой F(A"t,C) дает минимальный отклик. Если разница в значениях оценки F для нескольких областей минимальна или отсутствует, то проверяются соответствующие им области на смежных мозаиках A"t-1, A"t+1 и вычисляется комплексная оценка.

Научный руководитель – к.т.н., доц., А.А. Краснопольский

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 004.932

В.Д. Кирилюк

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

ВИКОРИСТАННЯ ГВИНТОКРИЛІВ DRONE В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

На сьогоднішній день системи відеонагляду відіграють дуже важливу роль в системах безпеки, і дають можливість спостерігати за заданим об'єктом постійно. Це суттєво зменшує використання людського фактору, що потребує великих затрат небезмежних ресурсів.

З розвитком Інтернету відбувся значний прорив в системах відеоспостереження, адже з'явилася можливість спостерігати за об'єктом або дією людей на цих об'єктах майже з любої точки Земної кулі. Достатньо тільки щоб був доступ до мережі Інтернет. Але система відеонагляду за допомогою відеокамер не ідеальна. Відеокамери охоплюють невелику площу та дистанційно пересуватися з місця на місце не можуть. Тобто стає проблемою контролювати територію, на якій знаходиться велика кількість об'єктів, бо потрібна велика кількість відеокамер, як біля об'єктів, так і по периметру. Тому сьогодні часто використовуються патрулі, що є економічно не раціональними. Поставлену задачу відео нагляду за периметром можна вирішити за допомогою використання гвинтокрила Drone.

Спереді знаходиться веб камера що демонструє на пристрій зображення в реальному часі. Також ще одна веб камера знаходиться знизу, для контролю ситуації. Також знизу знаходиться контакт для програмування дрону. Програмування здійснюється через комп'ютер на базі linux.

Drone підключається по захищеному каналу wi-fi з одним девайсом. Всі інші ігнорує. Тим самим перехопити його неможливо. Інформацію з камер він також передає по цьому захищеному каналу. Яку можна потім накопичувати у сервері.

В цому гвинтокрилі зібрано потужний процесор, що програмується. Тим самим він може виконувати різноманітні запрограмовані дії не гірше комп'ютера. Наприклад сканувати та аналізувати периметр, звіряти обличчя з базою даних, адаптуватися до погодних умов, реагувати на зовнішні подразники. Після чого передавати отримані данні до дистанційного пульта та на сервер. Але серед цих всіх переваг є і один недолік. Це малий час автономної роботи - 20 хв. Що може бути вирішена сьогоднішніми розробками у сфері бездротових підзарядних станцій.

Отже квадрикоптер Drone може суттєво допомогти у системі відеонагляду. Чим зекономить ресурси та зможе надати можливість управління та контролю майже з любого місця на планеті.

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

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 004.896:004.056.53

Стеценко О.В., Харченко І.В.
Національний авіаційний університет
oksanella@i.ua

ОДНОШАРОВИЙ ПЕРСЕПТРОН В СИСТЕМАХ РОЗПІЗНАВАННЯ ПІДПИСІВ ТА ВІДБИТКІВ ПАЛЬЦІВ

В часи розвитку новітніх технологій важко представити життя без надсучасних гаджетів, розміром з долоню, що дають необмежені можливості користувачеві в будь-якій точці планети. Окрім великих можливостей в користуванні також виникає спокуса доступу до забороненої інформації. Тому системи захисту інформації повинні крокувати в ногу з технологіями.

Незважаючи на скептицизм багатьох видатних людей та широкого загалу, обертів набирає розвиток штучних нейронних мереж – математичних моделей, а також їхніх програмних та апаратних реалізацій, побудованих за принципом функціонування біологічних нейронних мереж — мереж нервових клітин живого організму. Однією з перших моделей штучних нейронних мереж став персептрон. Імітація роботи мозку для розпізнавання рукописного тексту чи відбитку пальців може бути реалізована за допомогою одношарового персептрона з навчанням «без вчителя». Вхідними даними для роботи слугує масив значень {-1;1}, де {-1} позначає порожній (не зафарбований) піксель поля введення, а {1} – зафарбований піксель. Кожному елементи вхідного масиву відповідає його ваговий коефіцієнт. Навчання «без вчителя» означає, що під час запам’ятовування (навчання) зразкового символу (відбитку), вагові коефіцієнти збільшуються або зменшуються (залежно від вхідного значення) на одну й ту саму константу. Для порівняння тестового символу (відбитку) зі зразком використовується порогове значення

$$S = \cdot \sum_{i=} \quad ,$$

де

$$w_i^j = \begin{cases} \\ \end{cases} \quad = \quad - \quad \text{чання}$$

$$p - \quad \text{ий відсоток}$$

Відсоток у ваговому коефіцієнті передбачає не ідеальність кожного підпису чи похибку при зчитуванні відбитку пальця. На виході із персептрона ми отримуємо один із двох можливих результатів – заборону або дозвіл на доступ до інформації. Не зважаючи на простоту даної штучної нейромережі, її програмна реалізація є ефективною для використання у системах технічного захисту інформації, зокрема, для систем розпізнавання почерку або відбитків пальців.

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

ЗБІРНИК ТЕЗ

науково-практичної студентської конференції
«ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

14-15 березня 2016 р.

Київ

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