Донецкий национальный технический университет

Южный федеральный университет

МАТЕРИАЛЫ

Четырнадцатого международного научно-практического семинара

«ПРАКТИКА И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПАРТНЕРСТВА В СФЕРЕ ВЫСШЕЙ ШКОЛЫ»

ТОМ 2

15 – 18 апреля 2013 года

г.Донецк

Донецк - Таганрог

Донецкий национальный технический университет

Южный федеральный университет

«ПРАКТИКА И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПАРТНЕРСТВА В СФЕРЕ ВЫСШЕЙ ШКОЛЫ»

Материалы

Четырнадцатого международного научно-практического семинара

15 – 18 апреля 2013 года

г.Донецк

ТОМ 2

Донецк – Таганрог 2013

УДК 004.056

СИСТЕМА АНАЛІЗУ ПОТОКІВ ДАНИХ КОРИСТУВАЧІВ ІЗ ЗОВНІШНІХ USB-ПРИСТРОЇВ

Ковальов С.О., Кравченко О.Г., Цололо С.О., Варавка А.М.
ДонНТУ, м. Донецьк, Україна
Тел.: +380 (62) 301-07-23; E-mail: s.solos@gmail.com

Abstract: *The analysis of USB-devices features, architecture, operating principles and components are proposed. Algorithm of information security in corporate networks based on fuzzy search engines in user's USB data streams is developed. Article also describes ways to implement the features of the proposed algorithm as distributed software security system of user data streams from/to external USB-devices.*
Keywords*: USB, user data streams, fuzzy search, security system*

Актуальність завдання

Сучасні погрози в комп'ютерній безпеці можна поділити на дві групи: внутрішні та зовнішні IT-погрози. Поява поняття внутрішніх IT-погроз пов'язана з використанням операційних систем (ОС) для обробки конфіденційної інформації в корпоративних мережах. З урахуванням того, що в основі архітектури захисту сучасних універсальних ОС є принцип повної довіри до користувача, деякі ключові механізми захисту, що є вбудованими в сучасні ОС, не можуть забезпечити ефективної протидії внутрішнім IT-погрозам з боку інсайдерів – користувачів, допущених до обробки конфіденційної інформації в рамках виконання своєї службової діяльності. Санкціоновані користувачі несуть у собі найбільш імовірну погрозу крадіжки конфіденційних даних. Як наслідок, завдання контролю потоків даних сьогодні не вирішується вбудованими механізмами захисту ОС, тому його рішення повинне бути покладене на додаткові засоби захисту.

Для обміну інформацією між робочими станціями найбільш часто використовуються два основних способи. Перший з них є найбільш популярним і заснований на використанні мережевого підходу (електронна пошта, Інтернет, файлові сервери). Другий підхід передбачає обмін даними за допомогою зовнішніх накопичувачів, що підключаються до ПК по інтерфейсу USB (флеш-накопичувачі) [1]. І саме другий спосіб дуже часто використовується для збереження та передачі найбільш конфіденційної внутрішньої інформації, що не рекомендується до пересилання засобами Інтернету та електронної пошти. Саме контроль за потоками даних користувачів, що виникають при використанні другого способу передачі в з робочих станцій в корпоративних мережах, є важливим та актуальним завданням.

Таким чином, о*б'єктом дослідження* даної роботи є система контролю потоків даних користувача у корпоративних мережах, *предметом дослідження* є алгоритм фільтрації потоків даних користувача із зовнішніх пристроїв. При цьому головною *метою роботи* є організація контролю передачі даних для зовнішніх пристроїв, що підключаються за протоколом USB.

Алгоритм фільтрації даних

У роботі запропоновано реалізацію системи, що виконує функцію спостереження за робочими станціями співробітників будь якої організації чи підприємства. Кінцевою метою роботи і головною функцією системи є контроль інформації, яка переміщається співробітниками між накопичувачами робочих станцій та зовнішніми USB-носіями [2].

В основі системи знаходиться базовий алгоритм контролю і аналізу потоків даних із зовнішніх USB-пристроїв, який наведено на рис. 1.

Реалізація алгоритму контролю складається з кількох основних етапів:

1. *Аналіз пристроїв*, підключених до шини USB. У цій частині алгоритму визначаються параметри та характеристики пристроїв, які підключені до шини USB робочої станції користувача [3].

2. *Сканування портів на наявність* підключених пристроїв. Якщо пристрій знайдено, то формуються запити на отримання дескрипторів пристроїв для визначення типу пристрою. Якщо підключений пристрій є носієм інформації, то драйверу передається ідентифікатор пристрою.

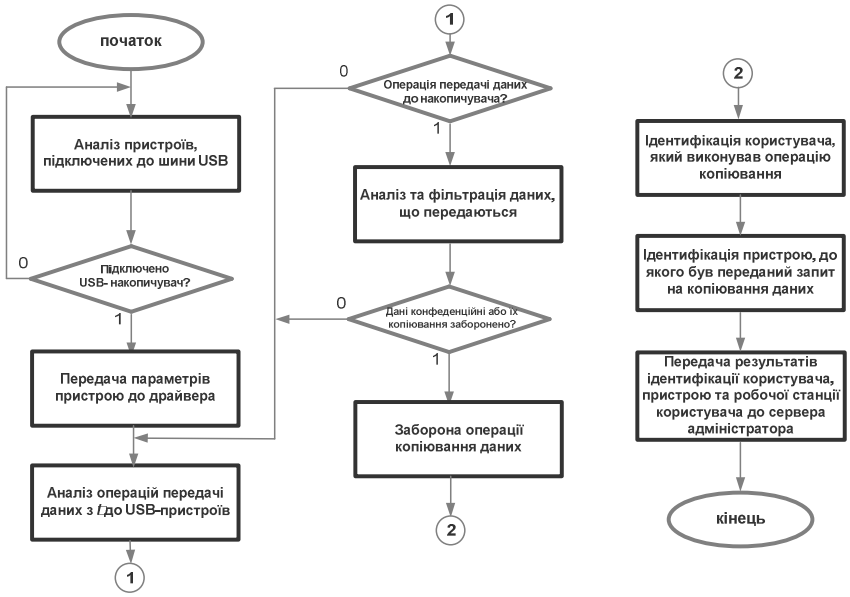

Рис. 1. Базовий алгоритм контролю і аналізу потоків даних із зовнішніх USB-пристроїв

3. *Аналіз операцій передачі даних з/до USB-пристроїв.* Функцію аналізу та контролю за виконанням операцій передачі даних до зовнішніх пристроїв виконує драйвер, який встановлено на робочій станції користувача. За допомогою драйвера здійснюється перехоплення функцій WinAPI, та існує можливість аналізу і контролю потоків даних користувача.

4. *Аналіз та фільтрація даних, що передаються.* Коли користувач формує запит на запис даних, драйвером аналізуються дані за вмістом, за іменами файлів та іншими параметрами, що задаються адміністратором. Якщо інформація є конфіденційною, то драйвером здійснюється заборона операції копіювання. В такому випадку здійснюється ідентифікація зовнішнього пристрою за декількома параметрами (фізична адреса робочої станції користувача, час виконання операції, серійний номер накопичувача та ін.).

Ключовим етапом алгоритму контролю є процес фільтрації, що складається з наступних етапів:

1. Отримання імені файлу від драйверу для подальшої фільтрації.
2. Завантаження словника у пам'ять модуля, який здійснює фільтрацію.
3. Перевірка розширення файлу і вибір відповідного конвертера.
4. Перетворення формату вхідного файлу в текстовий. На цьому етапі за допомогою визначеного конвертеру здійснюється перетворення файлу з поточного формату в текстовий для реалізації нечіткого пошуку.
5. Розбиття вмісту файлу за словами. Процедура розбиття вмісту файлу видаляє знаки пунктуації, після її виконання вміст текстового файлу являє собою послідовність рядків, що складаються зі слів і пропусків.
6. Порівняння слів, які містяться у вхідному файлі зі вмістом словника.
7. Підрахунок кількості збігів в результаті порівняння слів.
8. Аналіз результатів фільтрації та прийняття подальшого рішення.

Фільтрація даних за вмістом

Конфіденційна інформація на підприємстві, як правило, має свої характерні особливості. Для певних видів ділових паперів існує перелік ключових специфічних слів, фраз чи висловів, які властиві певним типам документів. Таким чином, є можливість за відомим фрагментом здійснювати фільтрацію потоків даних.

Для реалізації запропонованого методу фільтрації потоків даних можна використовувати *алгоритми нечіткого пошуку в тексті.* Нечіткий пошук являє собою важли-

вий механізм будь-якої пошукової системи. Разом з тим, його ефективна реалізація набагато складніша, ніж реалізація простого пошуку за точним збігом.

Алгоритми нечіткого пошуку характеризуються метрикою – функцією відстані між двома словами, що дозволяє оцінити ступінь їх подібності в даному контексті. Математичне визначення метрики включає в себе необхідність відповідності умові нерівності трикутника (X – безліч слів, p – метрика):

$$p(x, y) \le p(x, z) + p(z, y); x, y, z, \in X. \quad (1)$$

Як правило під метрикою мається на увазі більш загальне поняття – відстань. У числі найбільш відомих метрик – відстані Хеммінга, Левенштейна та Дамерау-Левенштейна. В розробленій системі використається саме цей набір метрік.

Відстань Хеммінга. Відстань Хеммінга – число позицій, в яких відповідні символи двох слів однакової довжини різні [4]. У більш загальному випадку відстань Хеммінга застосовується для рядків однакової довжини будь-яких q-ічних алфавітів і служить метрикою відмінності об'єктів однакової розмірності.

Відстань Хеммінга описується наступним чином:

$$d_{ij} = \sum_{k=1}^{p} \left| x_{ik} - x_{jk} \right|. \quad (2)$$

Відстань Хеммінга має властивості метрики, задовольняючи наступним умовам:

$$\begin{gathered} d(x, y) \ge 0; d(x, x) = 0, \\ d(x, y) = d(y, x); d(x, z) \le d(x, y) + d(y, z). \end{gathered} \quad (3)$$

Відстань Левенштейна. Відстань Левенштейна між двома рядками – це мінімальна кількість операцій вставки символу, видалення одного символу і заміни одного символу на інший, необхідних для перетворення одного рядка в інший [4].

Для розрахунку відстані Левенштейна найчастіше застосовують простий алгоритм, в якому використовується матриця розміром (N+1)*(M+1), де N і M – довжини порівнюваних рядків S_1 та S_2. Для конструювання матриці використовують таке рекурсивне рівняння:

$$d(S_1, S_2) = D(M, N) \quad (4)$$

$$D(i, j) = min\ (D(i, j-1)+1, D(i-1, j)+1, D(i-1, j-1)+C_{зміни}$$

$$C_{зміни} = \begin{cases} 0, \text{якщо } S_1[i] = S_2[j] \\ 1, \text{інакше} \end{cases} \quad (5)$$

Відстань Дамерау-Левенштейна. Модифікація вносить у визначення відстані Левенштейна ще одне правило – транспозиція (перестановка) двох сусідніх букв також враховується як одна операція, поряд зі вставками, вилученнями та замінами. Для конструювання матриці відстані Дамерау використовують рекурсивне рівняння:

$$D(i, j) = min\ (D(i, j-1)+1, D(i-1, j)+1, D(i-1, j-1)+C_{зміни}+C_{трансп}$$

$$C_{зміни} = \begin{cases} 0, \text{якщо } S_1[i] = S_2[j] \\ 1, \text{інакше} \end{cases} \quad (6)$$

$$C_{трансп} = \begin{cases} 0, \text{якщо } S_1[i] = S_2[j-1] \text{ та } S_1[i-1] = S_2[j] \\ \alpha, \text{інакше} \end{cases}.$$

Для реалізації алгоритму пошуку Дамерау є необхідність модифікації алгоритму знаходження звичайного відстані Левенштейна наступним чином:

–зберігати не дві, а три останні рядки матриці;

–увести відповідну додаткову умову – у разі виявлення транспозиції при розрахунку відстані також враховувати і її вартість.

Метод N-грам. Алгоритм N-грам є найбільш широко використовуваним тому, що має дуже просту реалізація, та забезпечує досить хорошу продуктивність. Алгоритм базується на принципі: «Якщо слово *А* збігається зі словом *Б* з урахуванням декількох помилок, то з великою часткою ймовірності в них буде хоча б один спільний підрядок довжиною N». Підрядки довжиною N називаються N-грамами [4]. Принцип розподілу слова на N-грами наведений на рис. 2.

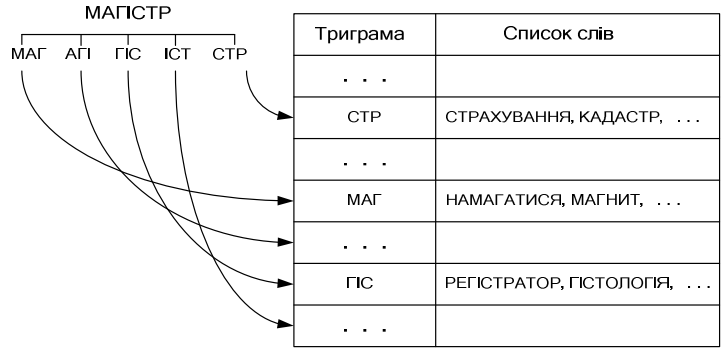

Рис. 2. Принцип розподілу слова на N-грами

Система контролю потоків даних користувачів

Система контролю потоків даних користувачів має клієнт-серверну архітектуру. За одним сервером може бути закріплено декілька клієнтів, але один клієнт не може працювати з декількома серверами. Сервер складається з одного програмного модулю, основними задачами якого є обмін даними з клієнтами та їх налаштування. Клієнтська частина має більш складну структуру, яка складається з трьох окремих модулів. Загальна структура програмного забезпечення системи наведена на рис. 3.

Перший модуль клієнтської частини виконує ініціалізацію системи, забезпечує обмін даними з серверною частиною та запускає наступні модулі. Цей модуль виконує автозапуск процесу при запуску операційної системи, завантажує усі конфігураційні файли до пам'яті, налагоджує взаємодію з серверною частиною.

Другий модуль реалізовано у вигляді драйверу ядра – головною функцією якого є перехват файлів, які модифікуються на змінному USB-носії та передача параметрів файлів до модулю аналіз даних. Драйвер – це ядро системи, без наявності цього модулю робота неможлива.

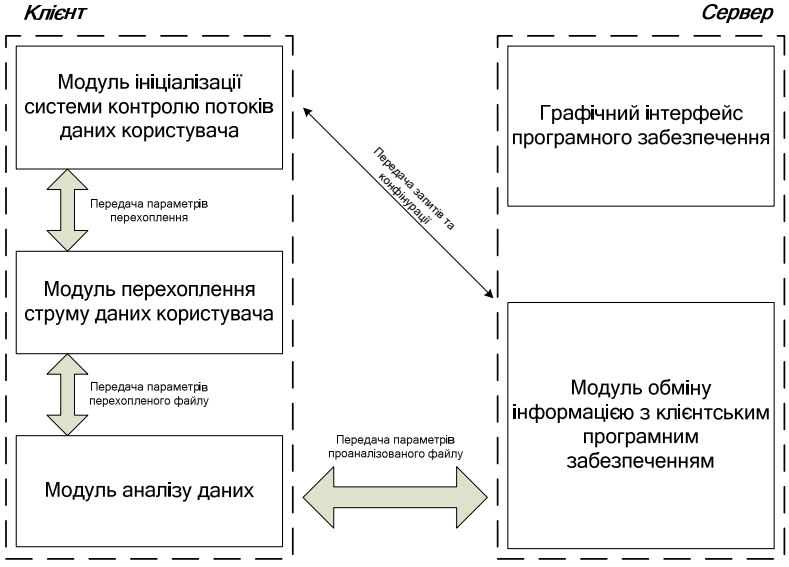

Рис. 3. Загальна структура системи контролю

Третій модуль – модуль аналізу вмісту файлів. До модулю аналізу драйвер передає інформацію щодо файлу, перетворює тип, який потрібен при виконанні аналізу та фільтрації, далі розпочинається детальний аналіз вмісту файлу. Наприкінці аналізу робиться висновок щодо безпеки цього файлу та приймається відповідне рішення про блокування, видалення або копіювання файлу.

Висновок

У роботі розглянуто рішення актуальної задачі організації контролю передачі даних для зовнішніх пристроїв, що підключаються за протоколом USB, в рамках створення комплексного засобу захисту конфіденційної інформації на підприємстві.

В роботі запропоновано алгоритм контролю, аналізу та фільтрації потоків даних із зовнішніх накопичувачів на основі алгоритмів нечіткого пошуку в тексті, які є основою процесу фільтрації інформації за вмістом. Для реалізації запропонованого алгоритму розроблена клієнт-серверна система контролю передачі потоків даних, що реалізує запропонований алгоритмі фільтрації даних за вмістом і може бути використана на реальному об'єкті.

В наступних роботах, що будуть пов'язані з розглянутою тематикою, автори планують докладно розглянути дослідження запропонованого алгоритму фільтрації та можливі засоби збільшення його ефективності і швидкодії.

Список літератури: 1. Агуров П. В. Интерфейс USB. Практика использования и программирования. – СПб: БХВ-Петербург, 2004. – 576 с. **2.** Варавка А.В. , Н.С. Демеш, Цололо С.А., Исследование алгоритма обеспечения информационной безопасности в компьютерных системах предприятий на базе интерфейса USB. Материалы VII международной конференции «Информатика и компьютерные технологии». – Донецк, ДонНТУ. – 2011. – С. 42-44. **3.** Варавка А.В., Цололо С.А. Идентификация USB-устройств в системе анализа пользовательских потоков данных. –Інформаційні управляючі системи та комп'ютерний моніторинг: III Всеукраїнська науково-технічна конференція, 16-18 квітня 2012 р. – Донецьк: ДонНТУ, 2012. – С. 371-475. **4.** Нечёткий поиск в тексте и словаре. [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/114997/.

УДК 681.3.016

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ ПРИБОРОВ LABVIEW ДЛЯ АНАЛИЗА РАБОТЫ ЦИФРОВЫХ СКРЕМБЛЕРОВ

Корниенко В.Т., Шеверева А.В.
ЮФУ, г.Таганрог, Россия
тел./факс 8 (8634) 371637

Abstract: *The design of LabVIEW's virtual devices of digital scrambler is considered.*
Key words*: digital scrambler, virtual device, pseudorandom numbers generators.*

Изучение разделов дисциплин «Физико-математичекие основы системотехники», «Инженерно-техническая защита информации» на кафедре РТС радиотехнического факультета ЮФУ сопровождается прививанием студентам практических навыков в построении технических средств, обеспечивающих защиту передаваемой информации в системах радиосвязи. Эта задача решается с использованием технологии создания виртуальных приборов в среде LabVIEW [1].

В средствах цифровой радиосвязи, где применимы методы криптографии, получившие широкое распространение, обеспечивая достаточно высокую степень защиты информации от несанкционированного доступа, также используются алгоритмы цифрового скремблирования, находящие применение при реализации методов потокового шифрования.

Целью работы является создание лабораторного практикума на основе технологии виртуальных приборов LabVIEW для выполнения скремблирования цифрового потока данных.

Известно, что цифровое скремблирование производит преобразование структуры цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности. Скремблер осуществляет защиту информации от несанк-

СОДЕРЖАНИЕ

Алєкперлі Ф.А., Шабанов М.А.
МОДЕЛЮВАННЯ ДІНАМИЧНИХ СІСТЕМ УПРАВЛІННЯ 3
Андриенко Е.В., Занин К.М., Панычев А.И.
МОДЕЛИРОВАНИЕ АНТЕННОЙ СИСТЕМЫ ТОЧКИ ДОСТУПА WLAN 6
Баркалов А.А., Зеленёва И.Я., Мирошкин А.Н., Товстоног А.А.
АВТОМАТИЗАЦИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ ЦИФРОВЫХ УСТРОЙСТВ УПРАВЛЕНИЯ 10
Баркалов А.А, Титаренко Л.А., Ефименко К.Н., Зеленева И.Я.
РАЗДЕЛЕНИЕ СХЕМЫ АДРЕСАЦИИ В КМУУ С ОБЩЕЙ ПАМЯТЬЮ 12
Борзов Д.Б., Корой В.В.
ВЫЯВЛЕНИЕ ПАРАЛЛЕЛИЗМА ВНУТРИ ЛИНЕЙНЫХ УЧАСТКОВ ПОСЛЕДОВАТЕЛЬНЫХ ПРОГРАММ, СОДЕРЖАЩИХ РЕКУРСИЮ И ВЫЗОВЫ ПОДПРОГРАММ, СО СВЯЗЯМИ ПО УПРАВЛЕНИЮ 18
Бровкина Д.Ю., Приходько Т.А.
РАЗРАБОТКА МОБИЛЬНОГО РОБОТА С ОПТИМАЛЬНОЙ СХЕМОЙ ПИТАНИЯ 20
Волощенко В.Ю.
ИМПУЛЬСНЫЙ ПАРАМЕТРИЧЕСКИЙ ИЗЛУЧАТЕЛЬ НА СТОЯЧИХ ВОЛНАХ КОНЕЧНОЙ АМПЛИТУДЫ 24
Геложе Ю.А., Клименко П.П., Максимов А.В.
УПРАВЛЕНИЕ ПРОЦЕССАМИ В ФАЗОВОЙ СИСТЕМЕ АВТОПОДСТРОЙКИ ЧАСТОТЫ ЦИФРОВЫХ СИНТЕЗАТОРОВ ЧАСТОТЫ В КРИТИЧЕСКИХ РЕЖИМАХ 26
Гришко Е.Е., Сапронова О.В., Паслён В.В.
МОДЕЛИРОВАНИЕ ШИРОКОПОЛОСНЫХ АНТЕНН С КРУГОВОЙ ПОЛЯРИЗАЦИЕЙ В ПРОГРАММНОМ ПРОДУКТЕ MMANA 29
Гусева М.Н., Евтушенко В.Ю., Скубилин И.М.
ОБРАБОТКА РЕЗУЛЬТАТОВ МОНИТОРИНГА СПОСОБНОСТИ КУРСАНТОВ 31
Долженкова В.В., Киреев Д.О., Звягинцева А.В.
ПЕРСПЕКТИВЫ ПРОСТРАНСТВЕННОГО АНАЛИЗА В ГИС СИСТЕМАХ ДЛЯ ПРОГНОЗИРОВАНИЯ РИСКА НАВОДНЕНИЙ 36
Дубинская И.В., Панычев А.И.
МОДЕЛИРОВАНИЕ ПРОХОЖДЕНИЯ ЧЕРЕЗ КОНСТРУКЦИИ ЗДАНИЯ СИГНАЛОВ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ СВЯЗИ 43
Заграй Н.П.
СПЕКТРАЛЬНЫЕ КОЭФФИЦИЕНТЫ МОЩНОГО СИГНАЛА В БИОСРЕДЕ С УЧЕТОМ НЕЛИНЕЙНОСТЕЙ ВЫСШИХ ПОРЯДКОВ 47
Захаревич В.Г., Ли В.Г., Комар А.В.
МЕТОДИКА ОЦЕНКИ ДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА-ОПЕРАТОРА РТС В СРЕДЕ ТМС ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ 51
Захарченко А.Д., Бокий И.А.
МОДЕЛИРОВАНИЕ РАБОТЫ ПЛОСКИХ РЫЧАЖНЫХ МЕХАНИЗМОВ 58
Касьянов А.О., Билан А.Н.
ЭЛЕКТРОДИНАМИЧЕСКАЯ МОДЕЛЬ МИКРОПОЛОСКОВО-ШТЫРЕВОЙ ОТРАЖАТЕЛЬНОЙ АНТЕННОЙ РЕШЕТКИ 62

Кисель Н.Н., Грищенко С.Г., Кардос Д.А.
МОДЕЛИРОВАНИЕ И ЧИСЛЕННОЕ ИССЛЕДОВАНИЕ АНТЕННОЙ СИСТЕМЫ БАЗОВОЙ СТАНЦИИ LTE СВЯЗИ 64
Кисель Н.Н., Грищенко С.Г., Мерглодов Д.В.
ОПЫТ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ «WIRELESS INSITE» ДЛЯ МАГИСТЕРСКОЙ ПОДГОТОВКИ ПО НАПРАВЛЕНИЮ "ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ" 67
Кисель Н.Н., Грищенко С.Г.
ЭЛЕКТРОДИНАМИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВЫСОКОЧАСТОТНЫХ УСТРОЙСТВ НА БАЗЕ НАУЧНО-ОБРАЗОВАТЕЛЬНОГО ЦЕНТРА «ЦЕНТР КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ И ЭЛЕКТРОННЫХ САПР АНТЕНН И УСТРОЙСТВ СВЧ» 70
Клевцова А.Б.
МОДЕЛЬ ПРОЦЕССА ФОРМИРОВАНИЯ ТРЕБОВАНИЙ НА ПАРАМЕТРЫ РАЗРАБАТЫВАЕМОГО ТЕХНИЧЕСКОГО ОБЪЕКТА 73
Клевцов С.И.
МОДЕЛЬ ОБНАРУЖЕНИЯ НЕШТАТНОЙ СИТУАЦИИ НА ОСНОВЕ МАТРИЧНОГО ПАРАМЕТРИЧЕСКОГО ПРЕДСТАВЛЕНИЯ О КОНТРОЛИРУЕМОМ ОБЪЕКТЕ 76
Клевцов С.И.
ОСОБЕННОСТИ ВИЗУАЛЬНОГО ПРОЕКТНОГО МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ОБРАБОТКИ ИНФОРМАЦИИ В РЕАЛЬНОМ ВРЕМЕНИ В СИСТЕМАХ СБОРА И ОБРАБОТКИ ДАННЫХ ДАТЧИКОВ 81
Ковальов С.О., Кравченко О.Г., Цололо С.О., Варавка А.М.
СИСТЕМА АНАЛІЗУ ПОТОКІВ ДАНИХ КОРИСТУВАЧІВ ІЗ ЗОВНІШНІХ USB-ПРИСТРОЇВ 85
Корниенко В.Т., Шеверева А.В.
ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ ПРИБОРОВ LABVIEW ДЛЯ АНАЛИЗА РАБОТЫ ЦИФРОВЫХ СКРЕМБЛЕРОВ 89
Корой В.В.
SSD НОСИТЕЛЬ ПОВЫШЕННОЙ ИЗНОСОСТОЙКОСТИ НА ОСНОВЕ ВЫБОРОЧНОЙ БУФФЕРИЗАЦИИ 93
Косенко О.В.
АНАЛИЗ МОДЕЛЕЙ ПРОИЗВОДСТВЕННО-ТРАНСПОРТНЫХ ЗАДАЧ 94
Котова М.В., Звягинцева А.В.
РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ В ВИЗУАЛЬНОЙ ОБЪЕКТНО-ОРИЕНТИРОВАННОЙ СРЕДЕ ПРОГРАММИРОВАНИЯ DELPHI-7 99
Кравчук Д.А., Немыкина А.В.
ПРИМЕНЕНИЕ СЛОЖНЫХ СИГНАЛОВ ПРИ СОЗДАНИИ ГИДРОАКУСТИЧЕСКИХ СИСТЕМ СВЯЗИ ДЛЯ МОНИТОРИНГА МОРСКОГО ШЕЛЬФА 104
Кравчук Д.А.
ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ ПО УПРАВЛЕНИЮ ПРОЦЕССОМ МОДОВОГО РАСПРОСТРАНЕНИЯ СИГНАЛА В МЕЛКОМ МОРЕ ДЛЯ СИСТЕМ ДИСТАНЦИОННОГО МОНИТОРИНГА МОРСКОГО ШЕЛЬФА 105
Ледовской М.И.
ВИРТУАЛЬНАЯ СЕТЬ ДЛЯ ДЕМОНСТРАЦИИ ТЕХНОЛОГИЙ 1С ПРЕДПРИЯТИЕ 108

Масюков И.И., Борзов Д.Б.
ПЕРСПЕКТИВЫ И ВАРИАНТЫ ПРИМЕНЕНИЯ МНОГОПРОЦЕССОРНОЙ ТЕХНИКИ В СОВРЕМЕННОЙ ЖИЗНИ 112
Миронов Д.А., Борзов Д.Б.
ВОЗМОЖНОСТИ РАСПАРАЛЛЕЛИВАНИЯ ПРОГРАММ И ПАРАЛЛЕЛЬНОЙ КОМПИЛЯЦИИ ДЛЯ МНОГОЯДЕРНЫХ ПРОЦЕССОРОВ 113
Набиев Р.Н., Шукюров С.С.
ТРЕНИЕ В СИСТЕМЕ МАГНИТНОЙ ЛЕВИТАЦИИ 114
Оводенко А.В.
МОДЕЛИ КОНТРОЛЯ, ДИАГНОСТИКИ И РАБОТЫ МНОГОПРОЦЕССОРНОЙ МАЖОРИТАРНОЙ ТОЛЕРАНТНОЙ К ОТКАЗАМ ИЗМЕРИТЕЛЬНО ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ 121
Оводенко А.В., Самойленко А.П.
КОНЦЕПЦИИ РАЗВИТИЯ СИНТЕЗА ВСТРОЕННЫХ СИСТЕМ КОНТРОЛЯ БЕЗОТКАЗНОЙ РАБОТЫ БОРТОВЫХ РАДИОЭЛЕКТРОННЫХ А.В. КОМПЛЕКСОВ 124
Панычев А.И., Захарова Е.В.
СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАСЧЕТОВ ИНТЕНСИВНОСТИ СИГНАЛОВ WLAN ВНУТРИ ПОМЕЩЕНИЯ 129
Панычев А.И., Сербин А.И.
МОДЕЛИРОВАНИЕ РАСПРЕДЕЛЕНИЯ СИГНАЛОВ WLAN ВНУТРИ ПОМЕЩЕНИЯ С ЦИЛИНДРИЧЕСКИМ ПРЕПЯТСТВИЕМ 134
Песоченко С.В.
МИКРОКОНТРОЛЛЕРНЫЙ ПРИБОР ДЛЯ КОНТРОЛЯ И ПРЕДОТВРАЩЕНИЯ ЗАСЫПАНИЯ ВОДИТЕЛЯ ЗА РУЛЕМ 138
Петров Н.С.
ОРГАНИЗАЦИЯ ПРИЁМА ВЫСОКОДИНАМИЧНОГО ПОТОКА ИНФОРМАЦИИ КОММУНИКАЦИОННЫМ МОДУЛЕМ РАСПРЕДЕЛЁННОЙ ИНФОРМАЦИОННОЙ МИКРОКОМПЬЮТЕРНОЙ СИСТЕМЫ 141
Пьявченко О. Н. Нечитайло Г. А.
ИНТЕЛЛЕКТУАЛЬНЫЙ МИКРОКОНТРОЛЛЕРНЫЙ КОММУНИКАЦИОННЫЙ МОДУЛЬ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ МИКРОКОМПЬЮТЕРНОЙ СИСТЕМЫ 146
Самойленко А.П., Рудь Д.Е.
МЕТОД ОЦЕНКИ ЗАГРУЗКИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ В УСЛОВИЯХ НАРУШЕНИЯ ОРДИНАРНОСТИ ИНФОРМАЦИОННОГО ПОТОКА 150
Скубилин М.Д., Алмасани С.А.
К ВОПРОСУ О ТЕСТИРОВАНИИ СЕРДЕЧНОЙ ДЕЯТЕЛЬНОСТИ 155
Скубилин М.Д., Коберси И.С., Аль Дулайми А.Н.
О МАССОМЕТРИИ ТРАНСПОРТНЫХ СРЕДСТВ 159
Скубилин М.Д., Стефаненко В.К., Четырешников А.А.
ОБ АВТОМАТИЧЕСКОМ ОГРАНИЧЕНИИ СКОРОСТИ АВТОТРАНСПОРТНЫХ СРЕДСТВ 162
Скубілін М.Д., Нагучєв Д.Ш., Набієв Б.Р.
ПРО ЕЛЕКТРОННИЙ КАМУФЛЯЖ ІНФОРМАЦІЇ 166
Соловьёв М.А., Полуянович Н.К.
УПРАВЛЕНИЕ ЭЛЕКТРОПРИВОДОМ ДЕФЛЕКТОРОВ СИСТЕМЫ КОНДИЦИОНИРОВАНИЯ ВОЗДУХА ДЛЯ НЕЙТРАЛИЗАЦИИ ВРЕДНЫХ ВЕЩЕСТВ 169

Финаев В.И., Скубилин М.Д., Коберси И.С., Каид В.А., Заргарян Ю.А.
К ВОПРОСУ О РАДИООБСЕРВАЦИИ 173
Финаев В.И., Скубилин М.Д., Одей Ф.О.
ОБ ОПТИМИЗАЦИИ В ЭЛЕКТРОЭНЕРГЕТИКЕ 178
ШушановИ.И., Полуянович Н.К.
ИССЛЕДОВАНИЕ ИМПУЛЬСНОГО РЕГУЛЯТОРА НАПРЯЖЕНИЯ 182
Barkalov A.A., Malcheva R.V.,Barkalov A.A.
REDUCTION IN THE NUMBER OF LUTS IN LOGIC CIRCUIT OF MEALY FSM 187
Kobersi I.S., Abdulmalik S., Shkurkin D.V.
COMPARE BETWEEN FLC AND PID REGULATORS IN THE OIL LEVEL CONTROL TASK 192
Kobersi I.S., Firov N.A., Sakhno D.A.
OPTIMIZATION GENETIC ALGORITHM OF NEURAL NETWORK IN THE TASKS OF VEHICLE PARKING 196
Malcheva R.V., Kovalev S.A., Mohammad Yunis
RESEARCH OF PRODUCTIVITY OF A PARALLEL INPLEMENTATION OF RAY-POLYGON INTERSECTION STAGE 199