

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

ВІСНИК

НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
“ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Видається з 1964 р.

№ 806

КОМП’ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ

Відповідальний редактор – д-р техн. наук, проф. А. О. Мельник

Львів
Видавництво Львівської політехніки
2014

УДК 621.3 (681, 519, 536, 62, 50, 003, 004)

Вісник Національного університету “Львівська політехніка” “Комп’ютерні системи та мережі” входить до переліку видань ВАК, в яких друкуються матеріали дисертаційних робіт у галузі технічних наук

У Віснику надруковані статті, що відображають результати досліджень з актуальних питань комп’ютерних систем, мереж та інформаційних технологій, виконаних науковцями Національного університету “Львівська політехніка”, вченими інших регіонів України в галузі теорії та розробки комп’ютерних систем, мереж та їх компонентів, комп’ютерних засобів розв’язування задач цифрової обробки сигналів, автоматизованого проектування та керування, захисту інформації.

Для наукових працівників, викладачів вищих навчальних закладів, інженерів, що спеціалізуються у галузі обчислювальних систем, комп’ютерних мереж, комп’ютерних засобів розв’язання задач цифрової обробки сигналів, автоматизованого проектування та керування, захисту інформації, а також докторантів, аспірантів та студентів старших курсів відповідних спеціальностей.

*Рекомендувала Вчена рада Національного університету “Львівська політехніка”
(протокол № 69 від 25.02.2014 р.)*

*Свідоцтво про державну реєстрацію друкованого засобу масової інформації
серія КВ № 13038-1922Р від 20.07.2007 р.*

Редакційна колегія:

проф., д-р техн. наук А. О. Мельник (відп. редактор);
проф., д-р техн. наук Р. Б. Дунець (заст. відп. редактора);
доц., канд. техн. наук Я. С. Парамуд (відп. секретар);
проф., д-р техн. наук О. В. Дрозд;
проф., д-р техн. наук С. А. Лупенко;
проф., д-р техн. наук А. Й. Наконечний;
проф., д-р техн. наук Я. М. Николайчук;
проф., д-р техн. наук В. М. Опанасенко;
проф., д-р техн. наук О. В. Поморова;
проф., д-р техн. наук В. П. Тарасенко;
проф., д-р техн. наук М. В. Черкаський;
проф. Зденек Пліва;
проф. Ведат Коскун;
проф. Єсус Церетеро;
проф. Таня Владімірова;
проф. Джіафу Ван;
проф. Малгожата Суханська;
проф. Георгій Тодоров;
доц., д-р техн. наук В. С. Глухов;
доц., д-р техн. наук В. А. Мельник

Адреса редколегії:

*Національний університет “Львівська політехніка”
вул. С. Бандери, 12, 79013, Львів-13
e-mail: visnykksm@polynet.lviv.ua*

ЗМІСТ

<i>Бакай О. В.</i> Особливості побудови системи та застосування криптографічного алгоритму AES	3
<i>Березко Л. О., Соколов С. Є.</i> Особливості проектування електронної біомедичної апаратури	10
<i>Березовський М. О., Дунець Р. Б.</i> Особливості програмування динамічно реконфігурованих процесорів.....	14
<i>Бочкарьов О. Ю., Голембо В. А.</i> Метод координації адаптивних вимірювально-обчислювальних процесів на основі відкладеної у часі інформаційної взаємодії.....	22
<i>Глухов В. С., Тріщ Г. М.</i> Оцінка структурної складності багатосекційних помножувачів елементів полів Галуа.....	27
<i>Гончар С. Ф., Леоненко Г. П., Юдін О. Ю.</i> Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури.....	34
<i>Горбенко Ю. І., Ганзя Р. С.</i> Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів	40
<i>Дудикевич В. Б., Микитин В. Г., Ребець А. І., Банах Р. І.</i> Системна модель безпеки безпроводних технологій зв'язку шифрування даних у WIMAX-системах.....	49
<i>Дунець Р. Б.</i> Підхід до класифікації комунікаційних середовищ мереж на кристалі.....	57
<i>Євсєєв С. П., Король О. Г.</i> Дослідження загроз методів двофакторної автентифікації	62
<i>Іванюк Х. Ю.</i> Захист інформації в системі підвищення компетентнісних характеристик та оцінювання рівня знань аудиторів.....	72
<i>Ігнатович А. О.</i> Метод адаптивної автентифікації користувачів в комп'ютерних мережах на основі біометричних даних.....	78
<i>Калашиніков М. В., Яковенко О. О., Кушніренко Н. І.</i> Вбудовування цифрових водяних знаків у аудіофайли зі стисненням без втрат	83
<i>Карпінський М. П., Чиж В. М., Балабан С. М.</i> Аналітичний метод дослідження величини зміни параметрів сигналів у бездротових сенсорних мережах	88
<i>Карпінський М. П., Яциковська У. О., Балик А. В., Александер М.</i> Атаки на відмову в обслуговуванні комп'ютерних мереж.....	94
<i>Кононова В. О., Харкянен О. В., Грибков С. В.</i> Оцінка засобів захисту інформаційних ресурсів	99
<i>Костів Ю. М., Максимович В. М., Гарасимчук О. І., Мандрона М. М.</i> Формування пуассонівської імпульсної послідовності на основі генератора Голлманна.....	105
<i>Кочан Р. В., Кочан О. В., Клим Г. І., Гоц Н. Є.</i> Метод корекції нелінійності АЦП на базі джерела підвищеної напруги	111
<i>Крет Т. Б.</i> Захист інформації в інтелектуальних системах керування.....	119
<i>Кузнецов О. О., Олійников Р. В., Горбенко Ю. І., Пушкарьов А. І., Дирда О. В., Горбенко І. Д.</i> Обґрунтування вимог, побудування та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів	124
<i>Лупенко С. А., Шаблій Н. Р., Лупенко А. М.</i> Компаративний аналіз моделей, методів та засобів аутентифікації особи в інформаційних системах за її клавіатурним почерком	141
<i>Луцків А. М., Вітрук І. А., Загородна Н. В.</i> Високопродуктивна інформаційна система алгебраїчного криптоаналізу потокових шифрів	148
<i>Мельник А. О.</i> Кіберфізичні системи: проблеми створення та напрями розвитку	154
<i>Мельник В. А., Кім А. Ю.</i> Операційні системи реконфігурованих комп'ютерів: будова і організація функціонування.....	162
<i>Мельник В. А., Лонім І. І.</i> Оптимізація відображення пам'яті програмних моделей спеціалізованих процесорів в архітектуру ПЛІС.....	168
<i>Мороз І. В., Ваврук Є. Я.</i> Критерії оцінювання відмовостійкості систем опрацювання сигналів	175

<i>Мулярович О. В., Голембо В. А.</i> Розроблення додаткового програмного модуля з використанням методів локальної оптимізації у комп'ютерній системі для розв'язання динамічної задачі комівояжера.....	181
<i>Назаркевич М. А., Троян О. А.</i> Розроблення програмного продукту для захисту інформації на основі плівок з прихованим латентним зображенням.....	187
<i>Николайчук Я. М., Касянчук М. М., Якименко І. З., Івасьєв С. В.</i> Ефективний метод модулярного множення в теоретико-числовому базисі Радемахера–Крестенсона.....	195
<i>Новосядлий С. П., Мельник Л. В.</i> Фізико-топологічні аспекти моделювання арсенідгалієвого супер-бета транзистора на гетероструктурах для швидкодіючих ВІС комп'ютерних систем	199
<i>Олійник Г. В., Грибков С. В.</i> Дослідження використання інтелектуального програмного комплексу для захисту комп'ютерних мереж.....	208
<i>Олещук О. В., Попель О. Є., Копитчук М. Б.</i> Метод вимірювання енергетичної ефективності обчислень на графічному ядрі.....	214
<i>Паралюх І. П.</i> Швидкодіючий подільник частоти із змінним коефіцієнтом ділення.....	221
<i>Прогонов Д. О., Куц С. М.</i> Варіограмний аналіз стеганограм, сформованих на основі комплексних методів приховання даних	226
<i>Пуйда В. Я., Мандзевич Н. Т.</i> Розробка структурної моделі мікропроцесорного ПД-регулятора.....	232
<i>Сало А. М., Кравець О. І.</i> Архітектура вендінгового автомату	240
<i>Самойленко Д. М.</i> Семантичні загрози мережному інформаційному ресурсу.....	247
<i>Селюх П. В.</i> Оцінка потужності множини модулів RSA, стійких до криптоаналізу.....	252
<i>Стефінко Я. Я., Піскозуб А. З.</i> Використання відкритих операційних систем для тестування на проникнення в навчальних цілях.....	258
<i>Тимощук П. В.</i> Аналіз моделі швидкісної аналогової нейронної схеми ідентифікації найбільших за значеннями з множини сигналів	263
<i>Тишик І. Я.</i> Широкозмугове опрацювання сигналів систем охорони.....	270
<i>Чекурін В. Ф., Притула М. Г., Химко О. М.</i> Методологія MES і комп'ютеризація управління ГТС	275
<i>Шологон О. З.</i> Обчислення структурної складності помножувачів у поліноміальному базисі елементів полів Галуа $GF(2^m)$	284
<i>Шологон Ю. З.</i> Оцінювання структурної складності помножувачів полів Галуа на основі елементарних перетворювачів.....	290
<i>Яковина В. С.</i> Моделювання параметра потоку відмов програмного забезпечення та визначення діапазонів показника його складності.....	296
<i>Nyemkova E.</i> Data protection of biometric authentication for remote access to a bank account.....	302
<i>Chaplyga V., Nyemkova E., Ivanishin S., Shandra Z.</i> Administration of access rights to the corporate network with the integrated automation of the bank	308

Збірник наукових праць

ВІСНИК
Національного університету
“Львівська політехніка”

Видається з 1964 р.

№ 806

**КОМП'ЮТЕРНІ
СИСТЕМИ ТА МЕРЕЖІ**

Редактори *Оксана Чернигевич, Ольга Дорошенко*

Комп'ютерне верстання *Олени Катачиної*

Художник-дизайнер *Уляна Келеман*

Здано у видавництво 02.11.2014. Підписано до друку 12.12.2014.

Формат 60×84¹/₈. Папір офсетний. Друк на різнографі.

Умовн. друк. арк. 36,7. Обл.-вид. арк. 29,2.

Наклад 100 прим. Зам. 141032.

Видавець і виготівник: Видавництво Львівської політехніки
Свідоцтво суб'єкта видавничої справи ДК № 4459 від 27.12.2012 р.

вул. Ф. Колесси, 4, Львів, 79013
тел. +380 32 2582146, факс +380 32 2582136
vlp.com.ua, ел. пошта: vmr@vlp.com.ua