Бовда Е.М., Терещенко В.И.
ОЦЕНКА НОРМЫ УПРАВЛЯЕМОСТИ ДОЛЖНОСТНЫХ ЛИЦ УЗЛОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ ОБРАБОТКИ ЭКСИЕРТНОЙ ИНФОРМАЦИИ
В статье дано определение нормы управляемости, приведена методика определения коэффициента загрузки и качества решения задач управления, дана оценка нормы управляемости при использовании экспертной информации о качестве выполнения функций должностным лицом.
Ключевые слова: норма управляемости, коэффициент загрузки, качество решения задач управления.

Bovda E., Tereshchenko V.
ASSESSMENT STANDARDS OFFICERS CONTROLLABLY UNITS INFORMATION TELECOMMUNICATION NETWORK BASED ON INFORMATION PROCESSING EXPERT
The article defines rules of control disclosed a method of determining the load factor and a solution of control problems, assess standards of control using expert information on the quality of official functions.
Keywords: norm manageability, load factor, quality control problem solving.

УДК 681.261.3

Максимович В.М., Шевчук М.С. [1]
Мандрона М.М. [2]
[1] Національний університет «Львівська політехніка»
[2] Львівський державний університет безпеки життєдіяльності

ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ГЕНЕРАТОРА ДЖИФФІ

У статті представлені результати дослідження генераторів Джиффі при різних базових регістрах зсуву з лінійними зворотними зв'язками (linear feedback shift registers - LFSR) і різній степені їх твірних поліномів, що проводилось з використанням статистичних тестів NIST. Отримані результати дають змогу оптимізувати параметри генератора при заданих параметрах вихідної псевдовипадкової послідовності.
Ключові слова: псевдовипадкова бітова послідовність, генератори псевдовипадкових чисел, статистичні характеристики.

Актуальність. Генератори псевдовипадкових чисел (ГПЧ) і псевдовипадкових бітових послідовностей (ГПВБП) використовуються у багатьох галузях техніки, зокрема, в системах захисту інформації для побудови потокових шифрів, в вимірювальній техніці, для імітації випадкових процесів. При цьому вимоги до їх технічних характеристик відрізняються в залежності від мети їхнього застосування.

Генерування псевдовипадкових послідовностей та перевірка на випадковість згенерованої послідовності є одною з важливих проблем сучасної криптології. У сучасних криптосистемах генератори псевдовипадкових послідовностей використовуються для створення ключової інформації та забезпечення параметрів цих систем.

При реалізації криптографічних перетворень використовують різні псевдовипадкові послідовності. Стійкість криптоперетворень безпосередньо залежить від алгоритму формування псевдовипадкових чисел та послідовностей [1].

Метою роботи є використання статистичних тестів Національного інституту стандартів і технологій (НІСТ) США (NIST – National Institute of Standards and Technology) [2] для дослідження якості генераторів псевдовипадкових бітових послідовностей на основі генератора Джиффі.

Генератори псевдовипадкових бітових послідовностей на основі генератора Джиффі

Спрощена структурна схема генератора Джиффі наведена на рис. 1 [3]. До його складу входять три регістри LFSR1 – LFSR3 і мультиплексор MUX.

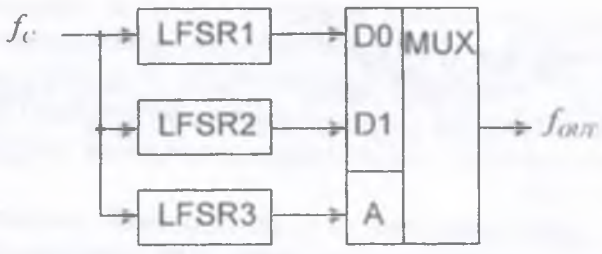

Рис. 1. Спрощена структурна схема генератора Джиффі

Генератор забезпечує перемішування двох імпульсних послідовносте з виходів LFSR1 і LFSR2 під керуванням послідовності з виходу LFSR3. У тому випадку коли значення періодів повторення вихідних послідовностей LFSR1, LFSR2, LFSR3 – T_{1p}, T_{1p}, T_{1p} попарно взаємно прості числа, період результуючою послідовності дорівнює добутку – $T_J = T_{1p} \cdot T_{2p} \cdot T_{3p}$ [3].

Нами були досліджені кілька варіантів побудови генератора Джиффі, при різних твірних поліномах LFSR1, LFSR2 і LFSR3, що визначають його структуру, а саме:

$$F(x) = \begin{cases} x^{11} + x^2 + 1 \\ x^{12} + x^6 + x^4 + x^1 + 1 \\ x^{13} + x^4 + x^3 + x^1 + 1 \end{cases}$$ – варіант А;

$$F(x) = \begin{cases} x^{16} + x^{10} + x^3 + 1 \\ x^{11} + x^2 + 1 \\ x^{15} + x^1 + 1 \end{cases}$$ – варіант Б;

$$F(x) = \begin{cases} x^{20} + x^3 + 1 \\ x^{21} + x^2 + 1 \\ x^{25} + x^3 + 1 \end{cases}$$ – варіант В;

$$F(x) = \begin{cases} x^{20} + x^3 + 1 \\ x^{21} + x^2 + 1 \\ x^{35} + x^2 + 1 \end{cases}$$ – варіант Г;

$$F(x) = \begin{cases} x^{20} + x^3 + 1 \\ x^{25} + x^3 + 1 \\ x^{28} + x^3 + 1 \end{cases}$$ – варіант Д;

$$F(x) = \begin{cases} x^{20} + x^3 + 1 \\ x^{25} + x^3 + 1 \\ x^{35} + x^2 + 1 \end{cases}$$ – варіант Е.

Для всіх LFSR був вибраний тип матриці T_1 і степінь матриці $r = 1$ [3].

На рис. 2-7 наведені статистичні портрети вихідної послідовності досліджуваних генераторів Джиффі, отримані нри випадково вибраних фіксованих ночаткових установках регістрів.

Отже, у результаті дослідження статистичних характеристик ГПВБП, з'ясовано, що для варіантів А-Г побудови генератора, вихідна псевдовипадкова послідовність не проходить хоча б один тест NIST (рис. 2-5).

При варіантах Д і Е побудови (рис. 6-7), досліджений генератор проходить усі тести NIST STS. Результати тестів знаходяться вище межі 0,98 (червона пунктирна лінія) [4], що згідно вимог статистичного оцінювання за допомогою пакету NIST свідчить про достатню статистичну безпеку.

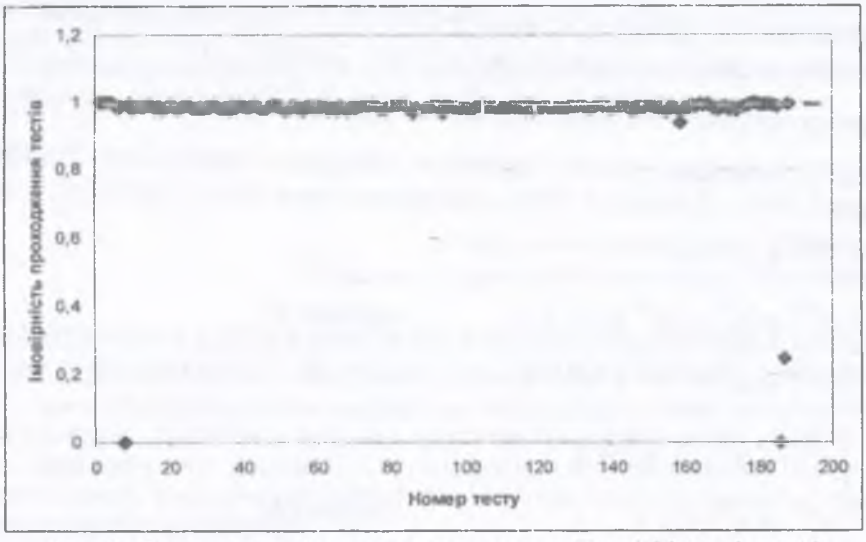

Рис. 2. Статистичний портрет генератора Джиффі (варіант А)

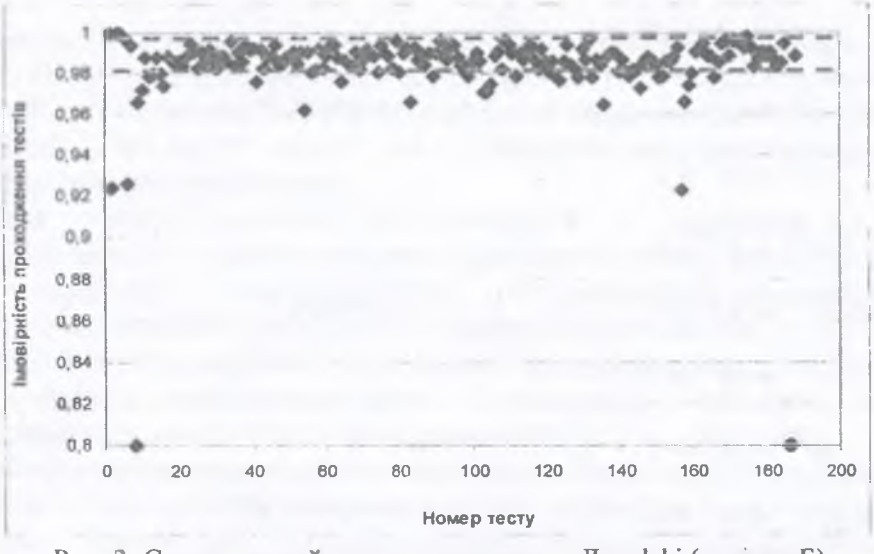

Рис. 3. Статистичний портрет генератора Джиффі (варіант Б)

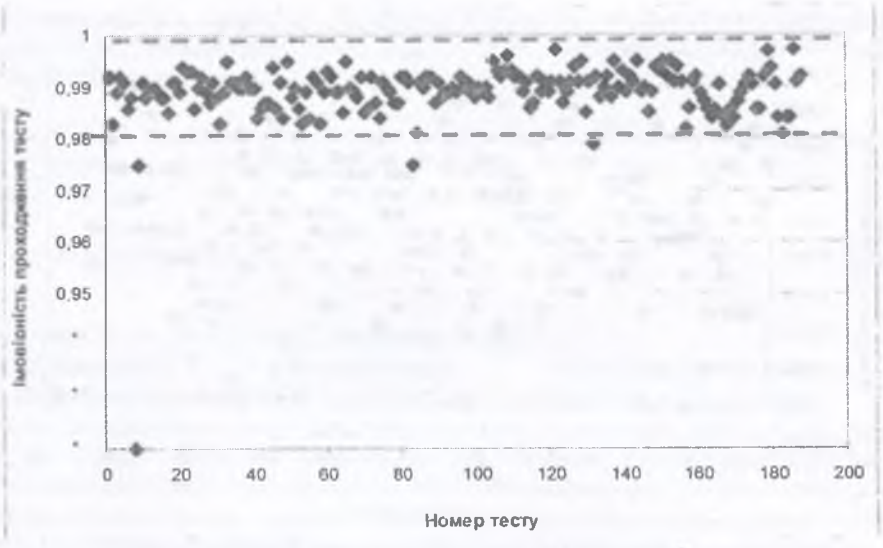

Рис. 4. Статистичний портрет генератора Джиффі (варіант В)

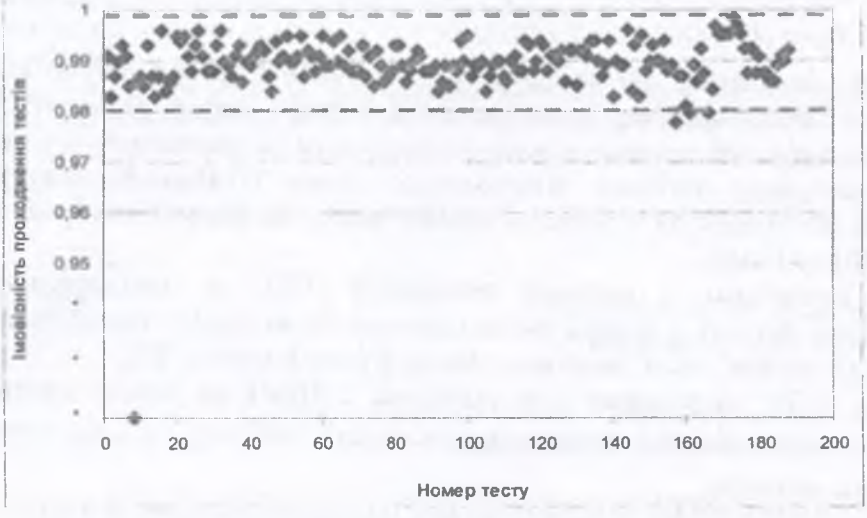

Рис. 5. Статистичний портрет генератора Джиффі (варіант Г)

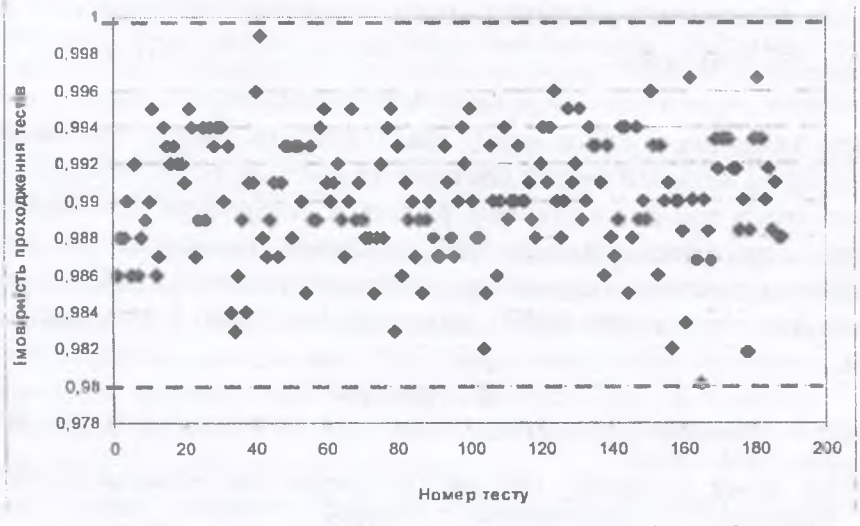

Рис. 6. Статистичний портрет генератора Джиффі (варіант Д)

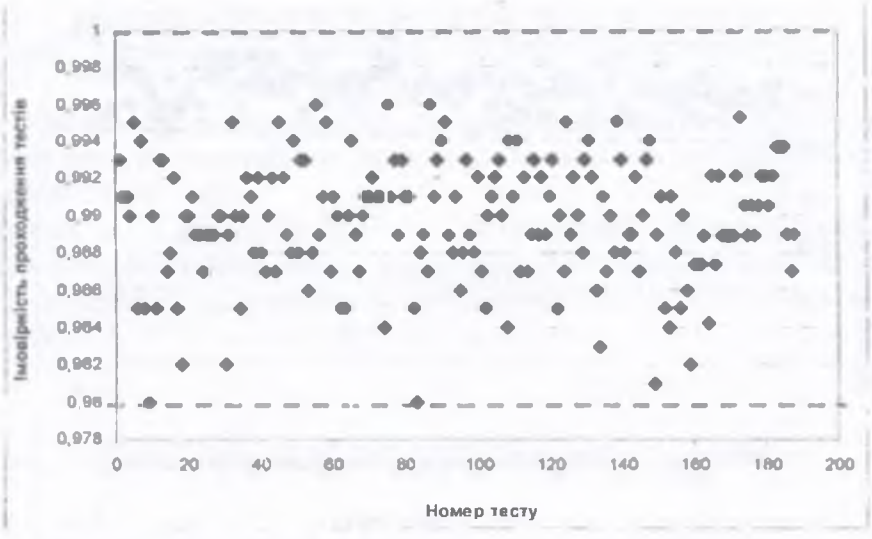

Рис. 7. Статистичний портрет генератора Джиффі (варіант Е)

Для усіх варіантів побудови генератора зафіксовано, що період повторення вихідної послідовності – $T_J > 10^9$.

Важливим фактором, що визначає якість ГПВБП, є складність його побудови – технологічність. Генератори, що розглядаються в даній роботі відносяться до цифрових апаратних генераторів, тобто пристроїв, що реалізуються на елементній базі цифрової техніки, зокрема, програмованих логічних інтегральних схемах (ПЛІС). У зв'язку з цим можна оцінювати технологічність за кількістю елементарних цифрових комірок, необхідних для побудови ГПВБП на ПЛІС.

Такими комірками, у випадку організації ПЛІС за архітектурою FPGA (Field Programmable Gate Arrays), є конфігуровані логічні блоки (КЛБ) призначені для виконання логічних функцій від декількох змінних, а також функцій пам'яті [5].

Кількість КЛБ, необхідних для побудови ГПВБП на основі генератора Джиффі, визначається сумарною кількістю розрядів усіх трьох LFSR – n_1, n_2, n_3, плюс один КЛБ для побудови мультиплексора:

$$A_{JIFFY} = n_1 + n_2 + n_3 + 1. \quad (1)$$

Криптографічним ключем ГПВБП на основі LFSR є початкові стани усіх трьох регістрів. Повна множина значень цих станів дорівнює $(2^{n_1} - 1) \cdot (2^{n_2} - 1) \cdot (2^{n_3} - 1)$, а довжина ключа визначається так.

$$C_{JIFFY} = n_1 + n_2 + n_3. \quad (2)$$

Висновки. Здійснене дослідження ГПВБП на основі генератора Джиффі показало, що навіть, не зважаючи на великий період повторення вихідної послідовності, при використанні малих значень степенів твірних поліномів регістрів, генератори не є повністю статистично безпечними, але збільшення степенів цих поліномів приводить до підвищення якості генератора. При певних визначених значеннях твірних поліномів ГПВБП на основі генератора Джиффі проходить усі тести NIST, що свідчить про його задовільні статистичні характеристики.

Література:

1. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

2. NIST SP 800-22. A Statistic Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application: [Електронний ресурс], April 2000. Режим доступу: http://csrc.nist.gov./publications/niatpubs//SP800-22rev1a.pdf.

3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванова, И.В. Чугунков. – М. : НИЯУ МИФИ, 2012. – 400 с.

4. Дослідження впливу параметрів генератора Голлманна на статистичні характеристики вихідного сигналу / [Мандрона М.М., Максимович В.М., Костів Ю.М., Гарасимчук О.І.] // Вісник кременчуцького національного університету імені Михайла Остроградського. – Кременчук: КрНУ, 2013. – Випуск 4 (81). – С. 98-103.

5. Мандрона М.М. Апаратні генератори псевдовипадкових бітових послідовностей з покращеними характеристиками : автореф. дис. на здобуття ступеня канд. техн. наук : спец. 05.13.21 «Системи захисту інформації». – Львів, 2015. – 24.

Рецензент: проф., д.т.н. Архіпов О.Є. Надійшла 25.10.2016

Максимович В.М., Шевчук М.С., Мандрона М.М.

ИССЛЕДОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ГЕНЕРАТОРА ДЖИФФИ

В статье представлены результаты исследования генератора Джиффи при различных базовых регистрах LFSR и разной степени их образующих полиномов, которые проводились с использованием статистических тестов NIST. Полученные результаты позволяют оптимизировать параметры генератора при заданных параметрах выходной псевдослучайной последовательности.

Ключевые слова: псевдослучайная битовая последовательность, генераторы псевдослучайных чисел, статистические характеристики.

Maksymovych V., Shevchuk M., Mandrona M.

RESEARCH OF PSEUDORANDOM BIT SEQUENCE GENERATOR BASED ON THE JIFFY GENERATOR

The article presents the results of jiffy generator estimation with a different number of basic LFSR generators, and different degrees of their polynomials, carried out with the use of NIST statistical tests. The received results allow optimizing the generator parameters at the given parameters of the output pseudorandom sequence.

Keywords: pseudorandom bit sequence, pseudorandom numbers generators, statistic characteristics.

УДК 629.039 : 351.749

Гончаренко Ю.Ю., Дивизинюк М.М.,
Касаткина Н.В., Камышенцев Г.В.[1]
Лазаренко С.В.[2]
[1]ГУ «Институт геохимии окружающей среды НАН Украины»
[2]Государственный Университет Телекоммуникаций

НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

На основании анализа особенностей критической инфраструктуры сформулированы основные подходы в обеспечении безопасности предприятий критической инфраструктуры от террористического воздействия. Они состоят в превентивности – заблаговременном обнаружении угрозы вторжения, оптимальном сочетании персонала охраны и используемых в охране технических средств, учете использования злоумышленниками самых современных достижений науки и техники.

Ключевые слова: обеспечение безопасности, чрезвычайная ситуация, злоумышленник, физическая защита, критическая инфраструктура.

Введение. Отсчет новой террористической волны в Европе следует вести от нападения француза Мехди Неммуша, застрелившего четырех человек в брюссельском Еврейском музее в мае 2014 года. В январе 2015 года была расстреляна редакция сатирического журнала Charlie Hebdo, высмеявшего фанатиков ислама. Его совершили представители "Аль-Каиды. 10 октября перед началом антивоенного митинга профсоюзов в столице Турции Анкаре произошли два мощных взрыва. Погибли 95 и ранены 246 человек. В Турции считают виновными террористов "Исламского государства" [1].

14 ноября 2015 года в столице Франции произошел ряд терактов. Несколько взрывов прогремели рядом со стадионом "Стад де Франс" во время матча между сборными Франции и Германии. Позже в парижском ресторане террористы совершили стрельбу. Погибли 140 человек. 22 марта в столице Бельгии произошло два взрыва в аэропорту Затем произошел

Інформаційна безпека

№3(23)
№4(24)
2016

Інформаційна безпека

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

№3 (23) 2016

№4 (24) 2016

НАУКОВИЙ ЖУРНАЛ

ЗАСНОВАНО У 2009 РОЦІ

ВИХІД З ДРУКУ – ЧОТИРИ РАЗИ НА РІК

ЗАСНОВНИК

Східноукраїнський національний університет ім. Володимира Даля

Журнал зареєстровано Міністерством юстиції України

Свідоцтво про державну реєстрацію **серія КВ №15063-3635Р**

Information security

VOLODYMYR DAHL EAST UKRAINIAN NATIONAL UNIVERSITY

№3 (23) 2016

№4 (24) 2016

THE FIRST ISSUE OF THE JOURNAL WAS PUBLISHED IN 2009

THE JOURNAL IS PUBLISHED QUARTERLY

FOUNDER

Volodymyr Dahl East Ukrainian National University

REGISTERED by the Ministery of Justice of Ukraine registration **sertificate KB №15063-3635P**

ISSN 2224-9613

До журналу увійшли статті студентів, аспірантів, докторантів Східноукраїнського національного університету імені Володимира Даля, вищих навчальних закладів України, Росії та закордонних країн.

Журнал підготовлено кафедрою безпеки інформаційних систем СНУ ім. В. Даля.

Рекомендовано до друку Вченою радою Східноукраїнського національного університету імені Володимира Даля (протокол №5 від 24.11.2016 р.).

Занесений до "Переліку фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук" ***з технічних наук***, затверджений постановою президії ВАК України від 14.05.2010 р., №1-05/3.

Матеріали номера друкуються мовою оригіналу.

ЗМІСТ ЖУРНАЛУ №4 (24) 2016

Айвазова К.Б.	АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ НОРМАТИВНОЇ ТА ЗАКОНОДАВЧОЇ БАЗИ УКРАЇНИ ДЛЯ ПОБУДОВИ ЗАХИСТУ АВТОМАТИЗОВАНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ	**73**
Молодецька-Гринчук К.В.	МЕТОДИКА ВИЯВЛЕННЯ МАНІПУЛЯЦІЙ СУСПІЛЬНОЮ ДУМКОЮ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ	**80**
Юрх Н.Г.	ОГЛЯД ІСНУЮЧИХ КАНАЛІВ ЗВ'ЯЗКУ	**93**
Опірський І.Р.	ПОСЛІДОВНА ПЕРЕВІРКА ДВОХ СКЛАДОВИХ ПРОГНОЗІВ В СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ МЕРЕЖАХ ПРИ НЕСТАЦІОНАРНОМУ КОРЕЛЬОВАНОМУ ГАУСІВСЬКОМУ СПОСТЕРЕЖЕННІ	**98**
Евсеев С.П.	СИНЕРГЕТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ БЕЗОПАСНОСТИ БАНКОВСКОЙ ИНФОРМАЦИИ	**104**
Вишнівський В.В., Василенко В.В., Гринкевич Г.О., Куклов В.М.	ІМПЛЕМЕНТАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ ХМАРНИХ ОБЧИСЛЕНЬ В РАМКАХ ЦЕНТРІВ ОБРОБКИ ДАНИХ	**118**
Бовда Е.М., Терещенко В.І.	ОЦІНКА НОРМИ КЕРОВАНОСТІ ПОСАДОВИХ ОСІБ ВУЗЛІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ ОБРОБКИ ЕКСПЕРТНОЇ ІНФОРМАЦІЇ	**125**
Максимович В.М., Шевчук М.С., Мандрона М.М.	ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ГЕНЕРАТОРА ДЖИФФІ	**130**
Гончаренко Ю.Ю., Дивизинюк М.М., Касаткина Н.В., Камышенцев Г.В., Лазоренко С.В.	НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА	**135**
Хорошко В.О., Хохлачова Ю.Є., Пірцхалава Л.Г.	ІСТОРІЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПОТИБОРСТВА. ЧАСТИНА 2.	**140**
Гнатюк С.О.	КІБЕРБЕЗПЕКА ЦИВІЛЬНОЇ АВІАЦІЇ УКРАЇНИ: АКТУАЛЬНІ ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ	**145**