

З М І С Т

Правове забезпечення захисту інформації.

Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення системи ТЗІ.

Стандартизація, сертифікація та випробовування засобів ТЗІ

МОДЕЛЬ ФАХОВОЇ СИСТЕМИ СТАНДАРТИЗАЦІЇ

Сергій Казанцев..... 6

СИСТЕМНІ АСПЕКТИ ОЦІНЮВАННЯ РІВНЯ ВАЖЛИВОСТІ СЕКРЕТНОЇ ІНФОРМАЦІЇ

Олександр Архипов, Валерій Ворожко..... 10

ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ ПЕРЕДБАЧЕННЯ ДЛЯ ОЦІНЮВАННЯ ШКОДИ, ЗАПОДІЯНОЇ ВИТОКОМ СЕКРЕТНОЇ ІНФОРМАЦІЇ

Олександр Архипов, Ігор Касперський 13

АНАЛІЗ РЕЗУЛЬТАТОВ ЕКСПЕРИМЕНТАЛЬНИХ АРТИКУЛЯЦІОННИХ ІССЛЕДОВАНИЙ МАСКИРОВАНОЇ ШЕПОТНОЇ РЕЧІ

Владимир Журавлёв, Александр Храмов, Сергей Завьялов..... 19

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ СКАНИРОВАНИЯ ИЗОБРАЖЕНИЙ

Михаил Глухимчук, Евгений Подгорный, Любовь Рябова..... 22

БЕЗПЕКА КІБЕРПРОСТОРУ ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ

Євген Скулиш, Дарія Прокоф'єва. 27

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТІВ ISO/IEC ТА УКРАЇНСЬКОЇ НОРМАТИВНОЇ БАЗИ В ЧАСТИНІ КЕРУВАННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сергій Гладіш, Володимир Кононович, Микола Тардаскін..... 31

ЗАДАЧИ ЭНЕРГЕТИЧЕСКОЙ И ЭНЕРГОИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА И ЧЕЛОВЕКА	
Ирина Кононович	39
АНАЛІЗ ЧУТЛИВОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДО ЗМІНИ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ЗАГРОЗ ТА КОЕФІЦІЄНТІВ МІЦНОСТІ МЕХАНІЗМІВ ЗАХИСТУ	
Олексій Новіков, Андрій Родіонов	46
Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах	
МЕТОД ПРИСКОРЕНОГО ЦИФРОВОГО ПІДПИСУВАННЯ НА ОСНОВІ МАТЕМАТИЧНОГО АПАРАТУ ЕЛІПТИЧНИХ КРИВИХ	
Юрій Яремчук, Костянтин Черняхович.....	50
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАВАДОСТІЙКОГО КОДУВАННЯ ДЛЯ АВТОМАТИЗАЦІЇ ВИЗНАЧЕННЯ КОГНІТИВНИХ ВЛАСТИВОСТЕЙ ІНФОРМАЦІЇ	
Сергій Троценко.....	56
АЛГОРИТМ МНОГОПРОГРАММНОЇ ГЕНЕРАЦІЇ ПАРОЛЬНОГО ДОСТУПА К ДАННИМ	
Георгій Кожевников, Татьяна Бондаренко.....	60
ЛИНЕЙНЫЙ СТОХАСТИЧЕСКИЙ АЛГОРИТМ ШИФРОВАНИЯ, БАЗИРУЮЩИХСЯ НА КАНОНИЧЕСКОМ РАЗЛОЖЕНИИ СЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ	
Игорь Атаманюк.....	63
АЛГОРИТМ ФОРМИРОВАНИЯ МАТРИЦ НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ ДЛЯ ПОСТРОЕНИЯ ПРОТОКОЛОВ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА, РЕАЛИЗУЮЩИХ ЗАДАННУЮ ИЕРАРХИЮ ДОСТУПА	
Андрей Волошин.....	67
ОЦІНКИ ЙМОВІРНОСТЕЙ УЗАГАЛЬНЕНИХ ЛІНІЙНИХ АПРОКСИМАЦІЙ РАУНДОВОЇ ФУНКЦІЇ ГОСТ-ПОДІБНОГО БЛОКОВОГО ШИФРУ	
Артур Шевцов.....	76

РЕАЛИЗАЦИЯ ПРОТОКОЛОВ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ
СТАНДАРТОВ ГОСТ 34.310–95 И ДСТУ 4145-2002

Лидия Гортинская, Николай Молдовян, Галина Козина 82

ТЕСТИРОВАНИЕ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ
ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ИСПОЛЬЗОВАНИЕМ КОНТЕКСТНОГО
МОДЕЛИРОВАНИЯ

Шарапов Виталий 86

**Забезпечення захисту інформації в системах зв'язку.
Технічні засоби системи захисту інформації**

ДОСЛІДЖЕННЯ КОНТРОЛЮ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ
ЗБЕРІГАННЯ FIBRE CHANNEL

Богдан Корнієнко, Семен Сулима 98

ВАРІАНТИ ЗАХИСТУ ВІД ЗАГРОЗ В КОМУНІКАЦІЯХ РОЗПОДІЛЕНИХ
МЕРЕЖ

В'ячеслав Василенко 104

4 Алфавітний покажчик 116