

З М І С Т

1 Правове забезпечення захисту інформації.

Проблеми розвитку нормативної та методичної баз системи захисту інформації.

Метрологічне забезпечення систем ТЗІ.

Стандартизація, сертифікація та випробовування засобів ТЗІ

НАПРАВЛЕНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ВОПРОСОВ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Владимир Гребнев, Алексей Скиба 6

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ВОПРОСЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ ЭЦП

Даниил Мялковский, Алексей Скиба 11

ОРГАНИЗАЦИЯ МЕЖЛАБОРАТОРНЫХ ИСПЫТАНИЙ

Евгений Володарский, Игорь Харченко 16

ЭФФЕКТИВНОСТЬ АДДИТИВНОЙ И МУЛЬТИПЛИКАТИВНОЙ КОРРЕКЦИИ ПОГРЕШНОСТЕЙ ПРИ ДИАГНОСТИРОВАНИИ

Елена Кириченко 20

2 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

КОЛИЧЕСТВЕННЫЕ ОЦЕНКИ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Денис Кудин, Владислав Корольков 25

ИСПОЛЬЗОВАНИЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПЬЮТЕРНЫХ СЕТЕЙ

Александр Хошаба 28

ИССЛЕДОВАНИЕ МЕТОДОВ КРИПТОАНАЛИЗА ПОТОЧНЫХ ШИФРОВ

Александр Потий, Юрий Избенко 34

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХАРАКТЕРИСТИК И ПРИНЦИПОВ ПОСТРОЕНИЯ СТАНДАРТОВ ЭЦП НА СВОЙСТВАХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Анатолий Кочубинский, Александр Шаталов 49

ПРИНЦИПЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ Анатолий Кочубинский	55
ВИКОНАННЯ ОПЕРАЦІЙ У ГРУПАХ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ НАД СКІНЧЕННИМИ ПОЛЯМИ Людмила Завадська, Анатолій Кочубінський	64
МЕТОД ГЕНЕРУВАННЯ ПАРАМЕТРІВ ЕЛІПТИЧНИХ КРИВИХ Микола Карпінський, Ігор Васильцов, Ігор Якименко, Ярослав Кінах	74
АЛГОРИТМ ОЦІНКИ ПАРАМЕТРІВ ОПТИМАЛЬНИХ КЛЮЧОВИХ СТРУКТУР, ПОБУДОВАНИХ НА ОСНОВІ НЕПОВНИХ УРІВНОВАЖЕНИХ БЛОК-СХЕМ Сергій Конюшок	79
СИСТЕМА ПЕРЕДАЧИ ИНФОРМАЦИИ СО СЛУЧАЙНЫМ КОДИРОВАНИЕМ, ПОСТРОЕННАЯ НА ОСНОВЕ КОДОВ РИДА-СОЛОМОНА Антон Алексейчук, Тарас Дроздовский, Юрий Сергиенко	84
ТЕСТИРОВАНИЕ ЧИСЕЛ НА ПРОСТОТУ: ТЕОРИЯ И ПРАКТИКА Иван Горбенко, Виталий Вервейко	89
3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації	
МЕХАНИЗМЫ И КРИТЕРИИ БЕЗОПАСНОСТИ СИСТЕМ БЕСПРОВОДНОЙ СВЯЗИ Евгений Гулак	97
ПУТИ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ РАДИОИНТЕРФЕЙСА В СЕТЯХ ОПОВЕЩЕНИЯ Александр Романов, Сергей Ливенцев, Игорь Столяр	106
ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ В УКРАИНЕ СИСТЕМ СОТОВОЙ СВЯЗИ 3-ГО ПОКОЛЕНИЯ Михаил Гряник, Георгий Карнаухов, Сергей Пасечник, Виктор Фролов	110
СИСТЕМЫ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА И МЕРЫ ПО ПРЕДУПРЕЖДЕНИЮ МОШЕННИЧЕСТВА В ОБЛАСТИ СОТОВОЙ ТЕЛЕФОННОЙ СВЯЗИ Алексей Марченков, Ярослав Бурьгин	112
СКОРОСТЬ СВЕТА: ОТ НУЛЯ ДО БЕСКОНЕЧНОСТИ Юрий Арепьев	120

4 Підготовка, перепідготовка та підвищення кваліфікації спеціалістів системи захисту інформації

ЗАДАЧИ И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ Александр Архипов, Валерий Ворожко	137
--	-----

МАТЕМАТИЧЕСКИЕ ОСНОВАНИЯ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ Михаил Савчук	140
--	-----

5 Короткі повідомлення

ВОЗМОЖНОСТИ АППАРАТНОЙ РЕАЛИЗАЦИИ ЭЛЕМЕНТОВ ДСТУ 4145-2002 Георгий Гусев	149
---	-----

СТАНДАРТИЗАЦИЯ ИНТЕРФЕЙСА И ФОРМАТА ДАННЫХ Алексей Остапченко	150
--	-----

ПРО НАПОВНЕННЯ ЗМІСТУ ПРОФІЛЮЮЧИХ НАВЧАЛЬНИХ ДИСЦИПЛІН СПЕЦІАЛІЗАЦІЇ “ЕЛЕКТРОННІ АПАРАТИ БАНКІВСЬКИХ СИСТЕМ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ” Юрій Зіньковський, Вадим Клименко	152
---	-----

6 Алфавітний покажчик	154
------------------------------------	------------