

СОДЕРЖАНИЕ

МЕТОДЫ СИНТЕЗА И АНАЛИЗА СИММЕТРИЧНЫХ ШИФРОВ

<i>Конюшок С.М., Олексійчук А.М., Сторожук А.Ю.</i> Швидкий імовірнісний алгоритм оцінювання відстані між зрівноваженою булевою функцією та множиною k -вимірних функцій	186
<i>Оліуныков Р., Kaidalov D.</i> Related-key cryptanalysis of perspective symmetric block cipher	192
<i>Кузнецов А.А., Иваненко Д.В., Колованова Е.П.</i> Моделирование перспективного блочного шифра «Калина»	201
<i>Лисицкий К.Е.</i> Снова об оптимальных S-блоках	208
<i>Горбенко И.Д., Долгов В.И., Лисицкий К.Е.</i> Уточнённые показатели прихода шифров к состоянию случайной подстановки	213
<i>Тимохин С.С., Горбенко И.Д.</i> Дослідження та порівняльний аналіз перспективних поточкових шифрів	217
<i>Долгов В.И., Лисицкая И.В., Лисицкий К.Е.</i> Новый взгляд на шифр Мухомор	221
<i>Кузнецов О.О., Иваненко Д.В., Колованова Е.П.</i> Аналіз колізійних властивостей режиму вироблення імітоставок із вибірковим гамуванням	226
<i>Руженцев В.И.</i> Вероятности двухцикловых дифференциалов gijndael-подобного шифра с произвольными подстановками	235
<i>Кузнецов О.О., Горбенко Ю.И., Колованова Е.П.</i> Періодичні властивості шифрдами у режимі output feedback	239

ЭЛЕКТРОННЫЕ ДОВЕРИТЕЛЬНЫЕ УСЛУГИ И ИХ РЕАЛИЗАЦИЯ

<i>Потий А.В., Горбенко Ю.И., Корнейко А.В., Козлов Ю.Н., Пушкарев А.И., Горбенко И.Д.</i> EIDAS: Принципы предоставления доверительных электронных услуг и проблема интероперабельности	252
<i>Горбенко Ю.И., Потий А.В., Костенко А.В., Исирова Е.В., Горбенко И.Д.</i> Состояние и сущность процессов нормализации Европейской нормативной базы в области электронных подписей	261
<i>Горбенко Ю.И., Ганзя Р.С.</i> Аналіз стійкості постквантових криптосистем	268
<i>Гончарова Ю.В., Ерёмченко А.А.</i> STORK – перспективный проект европейской транснациональной электронной идентификации	275
<i>Качко Е.Г., Балагура Д.С., Погребняк К.А.</i> Влияние свойств современных процессоров на производительность программ	281

КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ОЦЕНКА

<i>Бессалов А.В.</i> Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме	286
<i>Єсіна М.В., Горбенко І.Д., Бакликов О.О.</i> Пароль як фактор багатофакторної автентифікації	290
<i>Бойко А.О.</i> Метод протидії перебору паролів, що не створює вразливості порушення доступності	296
<i>Погребняк К.А., Денисов Д.С.</i> Загальна атака на NTRUEncrypt на основі помилок розшифрування	298
<i>Гриненко Т.А., Нарезжний А.П.</i> Применение кодов аутентификации сообщений для обнаружения модификаций данных в региональных системах дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС	301

МЕТОДЫ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ

<i>Потий А.В., Комин Д.С., Козлов Ю.Н.</i> Классификация методов обеспечения доверия к безопасности продуктов и систем информационных технологий	311
<i>Торба А.А., Бобух В.А., Бобкова А.А.</i> Быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования	316
<i>Горбачев В.А.</i> Достаточные условия безопасности информации в электронных системах	319
<i>Леншин А.В.</i> Метод проектування та верифікації функцій комплексів засобів захисту від несанкціонованого доступу	328
<i>Горбенко І.Д., Харламб М.І.</i> Порівняльний аналіз стандартизованих версій криптоалгоритму ECIES	333
<i>Броншпак Г.К., Громыко И.А., Доценко С.И., Перчик Е.Л.</i> Криптография нового поколения: интегральные уравнения как альтернатива алгебраической методологии	337
<i>Онацький О.В.</i> Методологія створення комплексної системи захисту інформації	350
<i>Рома О.М., Белас О.М., Ніколаєнко Б.А.</i> Імітаційна модель оцінки завадостійкості квазікогерентної демодуляції OFDM-сигналу під час обробки «в цілому»	357

Памяти Алмазова Владислава Борисовича (11.10.1932–04.10.2014)	364
--	-----