

СОДЕРЖАНИЕ

МЕТОДЫ И СРЕДСТВА АСИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

<i>Горбенко І.Д., Качко О.Г., Науменко Г.С.</i> Экспериментальне дослідження можливості використання параметрів NTRUPRIME для несимметричного шифрування згідно з стандартом ansi x9.98 - 2010	135
<i>Бессалов А.В., Олешко К.А., Поречная Д.Н., Цыганкова О.В., Черный О.Н.</i> Криптостойкие скрученные кривые Эдвардса с минимальной сложностью групповых операций	141
<i>Єсіна М.В.</i> Математична модель протоколу анонімного електронного підпису на основі ідентифікаційних даних	151
<i>Єсіна М.В., Кулібаба В.А.</i> Математична та програмна моделі реалізації атаки на зв'язаних ключах відносно механізму електронного підпису IBS-1	157
<i>Качко. Е.Г., Телевний Д.К.</i> Исследование возможности использования языков функционального программирования при моделировании методов криптографических преобразований	162
<i>Кузнецов О.О., Луценко М.С., Андрушкевич А.В., Мелкозерова О.М., Новікова Д.В., Лобан А.В.</i> Статистичні дослідження сучасних потокових шифрів	167

МЕТОДЫ И СРЕДСТВА СИММЕТРИЧНЫХ КРИПТОПРЕОБРАЗОВАНИЙ

<i>Родінко М.Ю., Олійников Р.В.</i> Математична модель оцінки властивостей неін'єктивних схем розгортання ключів симметричних блокових шифрів	179
<i>Руженцев В.И.</i> Проверка метода доказательства стойкости блочных шифров к атаке невыполнимых дифференциалов	184
<i>Торба А.А., Бобух В.А., Торба М.О., Торба А.О.</i> Детерминированные генераторы псевдослучайных последовательностей для потокового шифрования на основе ДЛРР	191

ПОСТКВАНТОВЫЕ И ЭЛЕКТРОННЫЕ ПОДПИСИ

<i>Ковальова Н.В., Горбенко Ю.І.</i> Аналіз постквантових механізмів електронних підписів на основі геш-функцій	195
<i>Пономар В.А., Бережний О.Г.</i> Швидкі алгоритми для обчислення ізогеній на еліптичних кривих	203
<i>Гармаш Д. В., Бакликов О. О., Філатова Н.В., Горбенко І.Д.</i> Квантові криптографічні алгоритми електронного підпису на основі мультіваріативних квадратичних перетворень	215

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

<i>Веклич С.Г., Лавровская Т.В., Рассомахин С.Г.</i> Статистическая модель функционирования системы передачи информации при использовании алгебраических методов обработки псевдослучайных кодов	226
<i>Стеценко П.І., Халімов Г.З.</i> Метод протидії атакам на таблиці маршрутизації на основі архітектур ботнетів для однорангової пірингової мережі Bitcoin	232
<i>Стеценко П.І., Перекопський О.О., Халімов Г.З.</i> Атака інфраструктури на однорангову пірингову мережу Bitcoin	240
<i>Полуянченко Н.А.</i> Поиск регистров сдвига с нелинейной обратной связью, формирующих последовательность максимального периода	245
<i>Краснобаев В.А., Кошман С.А., Янко А.С.</i> Методы оперативного контроля данных в системе остаточных классов, основанные на принципе параллельной нулевизации	253

Памяти Зеленского Александра Алексеевича (24.06 1943 – 15. 05. 2016).....	266
--	------------