

## СОДЕРЖАНИЕ

### **СИМЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ. СИНТЕЗ И АНАЛИЗ**

Олексійчук А.М. Суб'експоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правилами частинами .....	128
Лисицкая И.В., Долгов В.И. Блочные симметричные шифры и марковские процессы.....	137
Долгов В.И., Лисицкая И.В., Настенко А.А., Лисицкий К.Е. Оценки максимальных значений дифференциалов и линейных корпусов марковских шифров.....	144
Олейников Р.В., Кайдалов Д.С. Оценка сложности различения схемы Лей-Месси и случайной перестановки....	152
Руженцев В.И. О стойкости блочных шифров с rijndael-подобными преобразованиями к интегральным атакам .....	160
Бойко А.О., Халімов Г.З. Метод універсального гешування по раціональним функціям алгебраїчних кривих над кільцями .....	165
Кузнецов А.А., Король О.Г., Евсеев С.П. Исследование коллизионных свойств кодов аутентификации сообщений UMAS.....	171
Горбенко Ю.І., Хряпін Д.Е. Аналіз генератора псевдовипадкових послідовностей заснованого на багаторазовому гешуванні.....	184
Горбенко І.Д., Мордвінов Р.І. Порівняльний аналіз алгоритмів генерації псевдовипадкових послідовностей.....	188
Замула А.А., Семченко Д.А. Методы генерации псевдослучаных последовательностей и оценка их свойств.....	191

### **АСИМЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ. СИНТЕЗ, АНАЛИЗ, СВОЙСТВА, ПРИМЕНЕНИЯ**

Качко Е.Г., Балагура Д.С., Горбенко Ю.И. Обоснование и исследование практической реализации улучшенного алгоритма цифровой подписи NTRUSIGN .....	195
Горбенко І.Д., Макутоніна Л.В. Аналіз криптографічних алгоритмів на ідентифікаторах, що використовують алгебраїчні решітки .....	200
Паршина Д.А., Митяева И.А., Горбенко И.Д. Анализ криптографических систем в группах КОС .....	210
Бондаренко М.Ф., Балагура Д.С., Іваненко Д.В. Атака спеціального виду на NTRU .....	216
Аулов І.Ф., Горбенко Ю.І. Порівняльний аналіз криптографічних бібліотек з відкритим кодом та рекомендації з їх використання.....	220
Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей .....	225
Кутя Є.Ю., Горбенко І.Д. Аналіз, порівняння та особливості архітектури функції гешування blake проекту SHA-3 .....	228
Бессалов А.В., Чевардин В.Е. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой.....	234
Бессалов А.В. О некорректности стандартного условия для MOV-атаки на эллиптические кривые.....	238
Шевчук О.А. Схеми ЕЦП для груп підписів скорочених повідомлень.....	240
Кудин А.М. Однонаправленные функции с информационно невычислимой лазейкой.....	245

### **БИОМЕТРИЧЕСКИЕ ИСТОЧНИКИ ИНФОРМАЦИИ, ИХ АНАЛИЗ И ПРИМЕНЕНИЕ**

Винокурова Е.А. Проблемы компрессии данных большого объема в условиях неопределенности с целью выявления локальных особенностей .....	250
Горбенко І.Д., Олешко И.В. Метод оценки относительной энтропии и сравнительный анализ источников биометрической информации.....	255
Бугаєнко Х.А., Горбенко І.Д. Аналіз трьох біометричних методів автентифікації особи .....	262
Філоненко П.О., Барсуков Є.І., Винокурова О.А. Аналіз біометричних інтелектуальних методів автентифікації та ідентифікації особи за відбитками пальців та за голосом для захисту від несанкціонованого доступу.....	267

### **МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ**

Горбачев В.А. Формальные основы методов блокировки аппаратных закладных устройств .....	275
Мороз С.А., Краснобаев В.А., Замула А.А. Метод оперативного контроля данных в классе вычетов на основе использования позиционного признака непозиционного кода .....	281
Есин В.И., Есина М.В. Варианты использования операторов языка модели данных .....	288
Горбенко І.Д., Замула А.А. Синтез систем сигналов с заданными корреляционными свойствами, законами формирования, структурными и ансамблевыми свойствами .....	293
Потій О.В., Пилипенко Д.Ю., Гладкий Д.І. Властивості діяльності із забезпечення захисту інформації як системної категорії .....	299
Семёнов Д.В., Демченко Ф.Л. Метод оценки рисков нарушения информационной безопасности банковских учреждений.....	304
Єнгаличев С.О., Семенов С.Г. Біометрична автентифікація на основі аналізу клавіатурного почерку .....	309