

СОДЕРЖАНИЕ

ПЕРСПЕКТИВНЫЕ МЕТОДЫ ГЕНЕРАЦИИ КЛЮЧЕЙ И КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

<i>Лисицкий К. Е., Кузнецов А. А., Горбенко Ю. И., Оноприенко В. В., Стельник И. В.</i> Ускоренный метод вычисления алгебраической имунности нелинейных узлов замены симметричных шифров.....	81
<i>Кузнецов О. О., Білозерцев І. М., Пушкаръов А. І., Горбенко Ю. І., Онопрієнко В. В.</i> Дослідження методів формування випадкових нелінійних вузлів заміни симетричних шифрів	88
<i>Кузнецов О. О., Кіян А. С., Прокопович-Ткаченко Д. І., Зверев В. П., Котух Е. В. Кузнецова Т. Ю.</i> Періодичні властивості криптографічно стійких псевдовипадкових послідовностей	96
<i>Луценко М. С., Кузнецов О. О., Горбенко Ю. І., Пушкаръов А. І., Уварова А. О.</i> Генерація ключів з біометричних образів райдуужної оболонки ока.....	104
<i>Кузнецов А. А., Кіян А. С., Прокопович-Ткаченко Д. И., Зверев В. П., Котух Е. В., Кузнецова Т. Ю.</i> Доказуемо стойкий генератор псевдослучайных последовательностей для постквантового применения	115
<i>Елисеев Р. Ю., Родинко М. Ю., Олейников Р. В.</i> Дифференциальный криптоанализ блочного ARX-шифра «Кипарис-256»	121
<i>Горбенко І. Д., Качко О. Г., Пономар В. А., М. В., Акользіна О. С., Кулібаба В. А.</i> Аналіз сутності та моделі протоколу інкапсуляції ключів у кільці поліномів над скінченим полем.....	127
<i>Горбенко Ю. І., Кудряшов І. С., Науменко Д. С., Онопрієнко В. В.</i> Порівняння кандидатів електронного підпису на постквантовий стандарт NIST PQС на базі MQ-перетворень та функцій гешування	138
<i>Кравчук П. В., Горбенко І. Д., Пушкаръов А. І.</i> Аналіз застосування функції гешування у технології Blockchain	147

МЕТОДЫ И МОДЕЛИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

<i>Бессалов А. В.</i> 2-изогении полных и квадратичных кривых Эдвардса над простым полем	152
<i>Єсіна М. В.</i> Модель безпеки постквантових протоколів інкапсуляції ключів	160
<i>Конюшок С. М.</i> Метод розпізнавання k -вимірності булевих функцій, заданих за допомогою оракулів.....	168
<i>Есин В. И., Вилигура В. В.</i> Метод преобразования унаследованных баз данных в базу данных с универсальным базисом отношений	176
<i>Луценко М. С., Кузнецов О. О., Прокопович-Ткаченко Д. І., Зверев В. П., Уварова А. О.</i> Порівняльний аналіз біометричних криптосистем	182