Автореферат

Выпускная квалификационная работа бакалавра по направлению подготовки 01.03.04 «Прикладная математика» профиль «Математическое моделирование в экономике и технике» на тему: «Численная оценка качества случайных кодов длинной 256 бит по их близости к «белому» шуму в пространстве сверток Хэмминга, вычисленных по монотонно увеличивающимся значениям модулей».

Автор: Козинова А.А.

Научный руководитель от кафедры ВиПМ: к.т.н., доцент Тарасов Д.В.

Научный руководитель от АО «ПНИЭИ»: Юнин А.П.

Актуальность и цели. Нейросетевые преобразователи, используемые в биометрии, прежде всего, должны минимизировать энтропию примеров образов «Свой» и обеспечивать хэширование выходного кода. Целью работы является синтез метода быстрой оценки энтропии ключа длиной 256 бит, используемого далее при обучении нейросетевого преобразователя биометрии алгоритмом ГОСТ Р 52633.3-2011.

Материалы и методы. Вычисление энтропии по Шеннону приводит к задаче с экспоненциальной вычислительной сложности. По этой причине возникает близость кодов к «белому» шуму в пространстве с метрикой Хэмминга ГОСТ Р 52633.3-2011. Предложено повысить качество оценки случайных кодов за счет вычисления сверсток Хемминга во множестве систем счисления. Это позволяет создать 256 новых тестов качества случайной последовательности, что на много больше 16-ти тестов NIST (Национального института стандартов и технологий США). Итогом работы является бесплатное программное обеспечение, позволяющее оценивать качество 256 битных случайных последовательностей по критерию их близости к идеальному «белому» шуму.

Ключевые слова: расстояние Хэмминга, идеальный «белый» шум, сверстки Хэмминга, спектр состояний.