

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет информационных
технологий и электроники

Специальность 10.05.03 –

Специализация -

Кафедра
«Информационная безопасность
систем и технологий»

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

АЛГОРИТМ ОЦЕНКИ КОРРЕЛЯЦИОННОЙ СЦЕПЛЕННОСТИ
256 РАЗРЯДОВ ВЫХОДНОГО КОДА НЕЙРОСЕТИ ДЛЯ ПРИМЕРОВ
БИОМЕТРИЧЕСКОГО ОБРАЗА «ЧУЖОЙ»

Студент

Руководитель

Нормоконтролёр

Рецензент ст. науч. сотрудник АО «ПНИЭИ»



Горбунов Кирилл Андреевич

Никитин В. В.

Иванов А. П.

Калашников Д. М.

Работа допущена к защите (протокол заседания кафедры от 25.06.21 № 16)

Заведующий кафедрой

С.Л. Зефирова

Работа защищена с отметкой удовлетворительно (протокол заседания ГЭК
от 29.06.21 № 13)

Секретарь ГЭК

А.П. Иванов

Пенза 2021

проверка
8 бакин

Содержание

Термины и определения.....	4
Обозначения.....	7
Введение	8
1 Обзор средств тестирования биометрической аутентификации	10
1.1 Обзор нормативной документации по биометрической аутентификации.....	10
1.2 Обзор методов биометрической аутентификации.....	19
1.3 Обзор средств тестирования биометрической аутентификации.....	23
1.4 Обзор среды моделирования «БиоНейроАвтограф».....	28
2 Оценка вероятности ошибок второго рода и энтропии выходных кодов преобразователя биометрия-код	30
2.1 Анализ высокоразмерного нейросетевого распознавания образов	30
2.2 Оценка вероятности ошибок второго рода	32
2.3 Тестирование в среде моделирования «БиоНейроАвтограф»	33
3 Оценка корреляционной сцепленности кодов откликов внутри двух групп образов «Чужой»	39
3.1 Оценка коррелированности выходного состояния преобразователей биометрия-код.....	39
3.2 Численный эксперимент оценки коррелированности ключей образов «Чужой»	39
4 Подтверждение результатов численного моделирования через меру Хемминга (методика Ратникова).....	47
4.1 Численный эксперимент оценки коррелированности ключей образов «Чужой» с использованием функции «Сумма значений переменной диапазона».....	48
5 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	53
Заключение.....	56
Список используемых источников	58
Приложение А (обязательное) Международные биометрические стандарты, действующие на территории РФ	61

Приложение Б (обязательное) Алгоритм численного эксперимента оценки корреляционной сцепленности между ключами от примеров образа «Сура»	65
Приложение В (обязательное) Алгоритм численного эксперимента оценки корреляционной сцепленности между ключами от примеров образа «Сура» в пространстве расстояний Хемминга	66
Приложение Г (справочное) Статья, принятая к публикации в сборнике научных статей по материалам III Всероссийской научно-технической конференции «Безопасность информационных технологий» (г. Пенза, 4 июня 2021 г.)	67

Термины и определения

Биометрический образ – уникальный образ человека (лицо, рисунок отпечатка пальца, рукописный автограф, голосовой пароль, рисунок радужной оболочки глаза и т.д.), имеющий высокую сложность (высокую размерность по числу контролируемых биометрических параметров).

Биометрический параметр – параметр, извлекаемый из биометрического образа путем предварительной обработки данных (очистки, центрирования, масштабирования) и последующего вычисления некоторого функционала, как правило, свертывающего данные всего примера в одно число.

Биометрический образ «Свой» – биометрический образ человека, параметры которого порождают с высокой вероятностью на выходах обученной нейронной сети код его личного криптографического ключа.

Биометрический образ «Чужой» – случайный биометрический образ, параметры которого порождают на выходах обученной нейронной сети случайный выходной код.

Биометрическая идентификация – это предъявление пользователем своего уникального биометрического вапараметра и процесс сравнения его со всей базой имеющихся данных. Для извлечения такого рода персональных данных используются биометрические считыватели.

Биометрическая аутентификация – процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путём преобразования этого образа в соответствии с заранее определённым протоколом аутентификации.

Единая биометрическая система – совместный проект Банка России и «Ростелекома», направленный на сбор биометрической информации и её использование для идентификации (в более строгом понимании – для аутентификации) пользователей финансовых услуг.

Нейросетевой преобразователь биометрия-код – преобразователь, заранее автоматически обученный преобразовывать многомерные континуумы

примеров биометрического образа «Свой» в почти однозначный выходной код криптографического ключа или длинного пароля доступа. Нейросетевые преобразователи биометрия-код являются хорошо исследованными искусственными нейросетевыми молекулами.

Ошибка первого рода – вероятность отказа в идентификации пользователю, находящемуся в базе данных. Иначе – вероятность того, что человек может быть не распознан системой.

Ошибка второго рода – вероятность ложной идентификации пользователя, отсутствующего в базе данных. Иначе – процентный порог, определяющий вероятность того, что один человек может быть принят за другого.

Состояние «белый шум» – нормальный случайный процесс с нулевым математическим ожиданием и автокорреляционной функцией. «Белый шум» является математической абстракцией

Стойкость к атакам подбора – показатель, определяющий число попыток подбора, необходимое злоумышленнику для получения на выходе преобразователя неизвестного ему кода доступа «Свой» при использовании для атаки заранее сформированной базы биометрических образов «Чужой».

Коэффициент корреляции – это статистический показатель зависимости двух случайных величин.

Математическое ожидание – одно из важнейших понятий в теории вероятности, означающее среднее значение случайной величины. Математическое ожидание случайного вектора равно вектору, компоненты которого равны математическим ожиданиям компонента случайного вектора.

Стандартное отклонение – Стандартное отклонение случайной величины, выборки, статистической совокупности, набора данных или распределения вероятностей – это квадратный корень из ее дисперсии.

Расстояние Хемминга – число позиций, в которых соответствующие символы двух слов одинаковой длины различны

Энтропия выходных кодов – мера хаотичности информации, неопределённость появления какого-либо символа первичного алфавита. При отсутствии информационных потерь численно равна количеству информации на символ передаваемого сообщения.

Обозначения

$P_1(.)$ – вероятность появления ошибок первого рода (ошибочного отказа в подтверждении основной гипотезы);

$P_2(.)$ – вероятность появления ошибок второго рода (ошибочного принятия альтернативной гипотезы);

$E(.)$ – математическое ожидание;

$\sigma(.)$ – стандартное отклонение;

$h(.)$ – расстояние Хэмминга;

$H(.,.)$ – энтропия кода;

$\oplus$ – сложение по модулю два.

Введение

В настоящее время в активно развивающейся сфере информационно-коммуникационных технологий обозначился целый ряд проблем. Одной из наиболее важной из них является надежная защита информации в открытом информационном пространстве и высоко достоверная локальная и дистанционная аутентификация пользователей.

Информационное общество предполагает активное использование Интернет ресурсов. Государственные и частные структуры создают на своих сайтах личные кабинеты пользователей. К сожалению, существующая практика парольной защиты доступа к личным кабинетам обладает существенной уязвимостью. Пользователи не способны запоминать длинные случайные пароли. Владелец информационного ресурса не может быть уверен в том, что к личному электронному кабинету получил доступ именно его хозяин.

Для усиления защиты доступа к электронным кабинетам в настоящее время разрабатываются технологии биометрической аутентификации личности путем преобразования личных биометрических данных человека в его криптографический ключ или длинный пароль доступа, используются рукописные парольные фразы [1], которые позволяют выделить порядка 416 биометрических параметров. Недостаток слишком «коротких ключей» полностью отсутствует у нейросетевых преобразователей биометрия-код [2].

Использование биометрических систем в бизнесе существенно поднимет уровень безопасности, способствует укреплению трудовой дисциплины на предприятии или в офисе.

Доверие к средствам высоконадежной биометрической аутентификации определяется результатами их тестирования, выраженными в форме гарантий производителя, подтвержденных при необходимости сертификационными документами.

Основными параметрами, характеризующим безопасность биометрической аутентификации, являются:

FAR – Коэффициент ложного пропуска (англ. False Acceptance Rate) – также именуется «ошибкой 2 рода» P_2 ;

FRR – Коэффициент ложного отказа (англ. False Rejection Rate) – также именуется «ошибкой 1 рода» P_1 ;

Уровень сложности фальсификации – это отражение объема усилий и затрат, которые потребуются компрометации системы (подмена реального биометрического признака человека).

Для полноценного становления будущих специалистов по информационной безопасности возникает потребность их обучения тестированию нейросети на ее стойкость к атаками подбора.

В данной работе затрагиваются описанные выше вопросы.

Целью ВКР является вычисление коэффициентов корреляции ключей длиной в 256 бит на выходах нейросети, полученных при возбуждении нейросети примерами одного биометрического образа «Чужой».

Для достижения данной цели необходимо выполнить следующее:

- обзор средств тестирования биометрической аутентификации;
- расчет оценки вероятности ошибок второго рода и энтропии выходных кодов преобразователя биометрия-код;
- рассчитать оценка корреляционной сцепленности кодов откликов внутри двух групп образов «Чужой»;
- подтвердить результаты численного моделирования через меру Хемминга (методика Ратникова).

1 Обзор средств тестирования биометрической аутентификации

1.1 Обзор нормативной документации по биометрической аутентификации

Исторически первой формой работы с биометрическими данными можно смело назвать сбор сведений о правонарушителях в рамках работы силовых ведомств. Отпечатки пальцев, например, – классическое доказательство при расследовании преступлений. Работая с подозреваемыми и осужденными, правоохранительные органы фиксируют рост человека, характерные приметы его внешности. При этом, если в обычных биометрических системах данные обезличиваются, то здесь, напротив, устанавливается точная связь измеренных параметров с конкретным человеком.

Первый массовый приход биометрии запустила 10 сентября 2013 г. компания Apple, представив публике встроенный в iPhone 5s считыватель отпечатков пальцев – Touch ID. Объем продаж за 2017 г. составил – 1,5 млрд шт., 11 % смартфонов на Яндекс маркете имеют встроенный отпечаток пальца.

Вторая веха – биометрические паспорта, содержащие электронный носитель информации – бесконтактный чип [3].

Начало выдачи биометрических загранпаспортов нового поколения в России соответствует времени принятия Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ – так что появление статьи 11 о биометрических персональных данных в нем не случайно. Удостоверение личности пользователя с помощью биометрии можно встретить и в корпоративной среде. Внутри одной организации проблемы FAR / FRR не столь существенны (поскольку сотрудников сравнительно немного), а выгоды вполне ощутимы: такая модель идентификации и аутентификации снимает ряд традиционных рисков.

Согласно Постановлению Правительства РФ от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и

хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» в Единой биометрической системе (ЕБС) используется сочетание двух параметров: данных изображения лица человека, полученные с помощью фото- и видеоустройств и данных голоса человека, полученные с помощью звукозаписывающих устройств.

При этом стоит заметить, что параметры выбраны не по причине их надежности (и тот, и другой имеют наименее благоприятные показатели FAR / FRR), а из-за простоты и доступности – для прохождения идентификации достаточно веб-камеры, которая есть в любом современном мобильном устройстве. Порядок работы с ЕБС прописан в законах, которые рассмотрены выше: клиент посещает банк, предъявляет паспорт, дает согласие на обработку биометрических персональных данных и сдает биометрические данные, после чего сотрудник организации увязывает полученный образец с учетной записью клиента в Единой системе идентификации и аутентификации (ЕСИА) и отправляет сведения в ЕБС [4].

В настоящее время Россия, США, Китай, страны Евросоюза активно занимаются развитием биометрии и ее стандартизацией.

В США в период с 1992 по 2013 г. создано более 100 национальных стандартов, регламентирующих требования к биометрическим технологиям. Часть из этих стандартов переведена в ранг международных через международный комитет по стандартизации ISO/IEC JTC SC37 (Biometric), который создан в 2002 г. Стандартизацию безопасной связи биометрии и криптографии осуществляет ISO/IEC JTC SC27 (Security techniques) [5].

В свою очередь часть из них гармонизирована в России техническим комитетом ТК 355 (Автоматическая идентификация) в лице 7-го подкомитета (Биометрическая идентификация) (приложение А).

В России активно развивается технология нейросетевого связывания биометрии с кодом ключа доступа [2]. В период с 2005 по 2012 г. под нейросетевую технологию создан комплекс стандартов ГОСТ Р 52633.X, устанавливающих требования к разработке и тестированию средств высоконадежной биометрической аутентификации.

ГОСТ Р 52633.0–2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации» устанавливает требования к процедурам обработки биометрической информации и преобразователям нечетких (неоднозначных) биометрических образов пользователя в его длинный пароль или ключ, используемый далее в одной из процедур высоконадежной криптографической аутентификации.

Стандарт распространяется только на средства высоконадежной биометрической аутентификации, производители которых заявляют значения вероятностей ошибочного пропуска «Чужого» менее 10^{-12} . Требования к средствам биометрической аутентификации с большей вероятностью ошибочного пропуска «Чужого» регламентируются системой международных стандартов, разработанных ISO/IEC JTC1 SC37. [6].

ГОСТ Р 52633.1–2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»

Для тестирования средств биометрической аутентификации необходимы базы биометрических образов «Свой» и «Чужой», размеры которых должны быть достаточными для подтверждения характеристик тестируемых средств.

Необходимые для достоверного тестирования размеры баз биометрических образов «Свой» малы, и формирование таких баз легко осуществимо, а для образов «Чужой» велики (10^{12} образов и больше). Соответственно процесс создания баз естественных биометрических образов «Чужой» является крайне длительным и трудоемким. Создать базы такого размера в короткие сроки невозможно. В связи с этим при тестировании

приходится ограничиваться усеченными базами естественных образов «Чужой» размерами 10^3 - 10^5 образов, непосредственно полученными с тестируемого средства аутентификации. Дополнять такие базы приходится естественными биометрическими образами «Чужой», ранее полученными при тестировании средств аутентификации с аналогичными биометрическими преобразователями. Кроме того, приходится увеличивать размеры тестовой базы за счет применения искусственно синтезированных (синтетических) биометрических образов.

В настоящем стандарте изложены требования по формированию баз естественных биометрических образов. Вопросы пересчета биометрических образов, полученных на одном биометрическом преобразователе, в данные другого биометрического преобразователя в настоящем стандарте не рассматриваются. Также не рассматриваются и вопросы создания баз синтетических биометрических образов. [7].

ГОСТ Р 52633.2–2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»

Настоящий стандарт устанавливает требования по формированию синтетических биометрических образов, которыми следует руководствоваться при пересчете биометрических образов, полученных при помощи первичных преобразователей того же типа, но с другими параметрами, и требования к размножению имеющихся естественных биометрических образов [8].

ГОСТ Р 52633.3–2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора»

Наиболее сложной частью задачи является тестирование стойкости обученных преобразователей биометрия-код к атакам подбора. Как правило, создать достаточно большой объем естественных биометрических образов по требованиям ГОСТ Р 52633.1 технически невозможно. По этой причине

приходится многократно увеличивать размеры тестовой базы биометрических образов за счет синтетических биометрических образов, созданных по ГОСТ Р 52633.2.

В общем случае задача автоматизированного тестирования стойкости преобразователя биометрия-код требует формирования очень больших баз тестовых биометрических образов и применения высокопроизводительных вычислительных средств с большим объемом памяти. Областью применения настоящего стандарта не является общий случай перебора всех возможных биометрических образов, настоящий стандарт распространяется только на тестирование программных средств аутентификации, в которых предусмотрена возможность реализации специальных условий упрощения задачи тестирования, а также предусмотрены специальные тестовые режимы наблюдения внутренних данных преобразователя биометрия-код. Для средств высоконадежной биометрической аутентификации, выполненных с аппаратной защитой внутренних данных, или для программных средств, не предоставляющих доступа к своим внутренним данным в специальных режимах тестирования, процедуры настоящего стандарта не могут дать численной оценки стойкости к атакам подбора [9].

ГОСТ Р 52633.4–2011 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа».

Настоящий стандарт представляет собой спецификацию архитектуры (далее – модель) программного интерфейса нейросетевых преобразователей биометрия - код доступа и определяет модель нейросетевого преобразования биометрических данных человека в выходной код, пригодную для использования в любой биометрической технологии.

Разработка настоящего стандарта связана с необходимостью спецификации взаимодействия биометрических систем с нейросетевыми преобразователями биометрия-код доступа, выполненными с учетом требований ГОСТ Р 52633.0.

Настоящий стандарт освещает три стороны взаимодействия биометрических систем с нейросетевыми преобразователями биометрия-код доступа:

1) специфицирует интерфейс взаимодействия с нейросетевыми преобразователями биометрия-код доступа различных производителей, использующих различные биометрические технологии;

2) указывает требования к параметрам биометрических образов, используемых для обучения, тестирования, извлечения выходного кода нейросетевых преобразователей биометрия-код доступа;

3) определяет формат представления нейросетевых биометрических контейнеров, используемых для обеспечения анонимности, конфиденциальности и обезличенности размещенных в них биометрических параметров [10].

ГОСТ Р 52633.5–2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».

В настоящем стандарте описывается алгоритм обучения, который одновременно обладает высокой устойчивостью и обеспечивает достаточно высокое качество обучения с учетом специфических требований к нейросетевым преобразователям биометрия-код доступа, сформулированным в базовом стандарте ГОСТ Р 52633.0.

Важнейшим аспектом доверия к средствам высоконадежной биометрической аутентификации является то, насколько качественно обучен нейросетевой преобразователь биометрия-код доступа. Процесс обучения каждого искусственного нейрона преобразователя биометрия-код доступа должен быть полностью автоматизирован и обеспечивать высокий уровень вероятности принятия биометрического образа «Свой» при низком уровне вероятности ошибочного принятия биометрического образа «Чужой», оцениваемой по ГОСТ Р 52633.3.

Не все известные алгоритмы обучения искусственных нейронов могут быть применены при обучении средств высоконадежной биометрической

аутентификации. Часть алгоритмов обучения искусственных нейронов неустойчива, и поэтому обучение с их помощью не может быть полностью автоматизировано. Другая часть алгоритмов обучения искусственных нейронов устойчива, но не дает необходимого качества обучения нейросетевого преобразователя биометрия-код доступа [11].

ГОСТ Р 52633.6–2012 «Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой».

Настоящий стандарт определяет требования к средствам высоконадежной биометрической аутентификации, имеющим индикаторы близости введенного биометрического образа к образу «Свой», которые, с одной стороны, помогают участнику процесса аутентификации получать информацию о своих ошибках в процессе ввода биометрических данных, а с другой стороны, не дают достаточной информации для упрощения атаки случайного подбора.

Обеспечиваемая средством биометрической аутентификации стойкость к атакам подбора тем выше, чем сложнее используемый биометрический образ «Свой». Сложный биометрический образ «Свой» может быть получен увеличением длины биометрического образа, выбором редкого образа или объединением нескольких простых образов. Усложнение биометрического образа вызывает рост числа ложных отказов во время процедуры аутентификации и увеличивает ее продолжительность. Для снижения трудоемкости ввода сложного (составного) биометрического образа желательно повторять ввод только тех его фрагментов, в которых имеются ошибки.

Для обнаружения ошибок во вводимых биометрических образах средства высоконадежной биометрической аутентификации должны быть дополнены индикаторами близости биометрического образа к биометрическому образу «Свой». При этом индикаторы не должны существенно компрометировать тайну биометрического образа «Свой». [12].

В настоящее время стандартизация в данной области подчинена Федеральному агентству по техническому регулированию и метрологии (Росстандарт).

В целях реализации Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации», повышения эффективности работ по стандартизации на национальном, межгосударственном и международном уровнях и по согласованию с заинтересованными организациями создан ряд Технических комитетов (ТК). Вопросами стандартизации нейросетевой биометрии занимаются:

ТК 098 «Биометрия и биомониторинг» организован приказом Росстандарта РФ от 06.03.2017 № 448 (до этого функции возлагались на ТК 355).

В рамках ТК 098 разрабатываются национальные стандарты в области биометрических технологий, машиносчитываемых паспортно-визовых документов, идентификационных карт с биометрическими данными и биомониторинга.

С 2014 г. ТК 098 представляет национальный орган по стандартизации РФ со статусом активного члена (P-member) в ИСО/МЭК СТК 1/ПК 37 «Биометрия» (ISO/IEC JTC 1/SC 37 «Biometrics»).

С 2017 г. ТК 098 представляет национальный орган по стандартизации РФ со статусом наблюдателя (O-member) в ИСО/МЭК СТК 1/ПК 17 «Идентификационные карты и устройства идентификации личности» (ISO/IEC JTC1/SC 17 “Cards and personal identification”) и в ИСО/МЭК СТК 1/ПК 27 «Методы и средства обеспечения безопасности информационных технологий» (ISO/IEC JTC 1/SC 27 «IT Security techniques»), в части тем по биометрии и машиносчитываемых паспортно-визовых документов.

ТК 362 «Защита информации» организован приказом Росстандарта РФ от 27 июня 2017 г. № 1422.

Целью деятельности ТК 362 является реализация Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» и иных нормативных правовых актов в области стандартизации, а также содействие

повышению эффективности работ по стандартизации в области защиты информации некриптографическими методами на национальном, межгосударственном (региональном) и международном уровнях.

ТК 026 «Криптографическая защита информации» организован приказом Росстандарта РФ от 9 июня 2017 г. № 1319.

За техническим комитетом закреплены объекты стандартизации, относящиеся к методам шифрования (криптографического преобразования) информации, способам их реализации, а также методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись, а также обязанности голосовать по проектам международных стандартов в части криптографической защиты информации.

ТК 164 «Искусственный интеллект» организован приказом Росстандарта РФ от 25 июля 2019 г. № 1732 с целью повышения эффективности работ по стандартизации в области искусственного интеллекта на национальном и международном уровнях.

1.2 Обзор методов биометрической аутентификации

Биометрическая идентификация – это предъявление пользователем своего уникального биометрического параметра и процесс сравнения его со всей базой имеющихся данных. Для извлечения такого рода персональных данных используются биометрические считыватели [4].

Классифицируют два основных метода биометрической идентификации – на основе статических образов и на основе динамических образов.

Статические биометрические образы. Метод основан на идентификации физиологических данных человека, не меняющихся на протяжении всей его жизни. Идентификация осуществляется по отпечаткам пальцев, по выражению лица, по радужной оболочке и сетчатке глаза, по линиометрии руки, по тепловым полям лица, по ДНК, на основе акустических характеристик уха, по узору вен.

Статический метод идентификации имеет следующие недостатки: транспарентность биометрического образа, его открытость, нереальность оптимизации биометрического образа по намерению самого пользователя.

Динамические образы характеризуются тем, что их достаточно сложно похоже повторить несколько раз, а отсюда и высокая вероятность появления ошибки второго рода P_2 (пропуска «Чужого»). Но в то же время они достаточно просто изменяются пользователем – легко меняется пароль (слово-фраза).

Аутентификации по рукописному почерку имеет преимущество перед аутентификацией пользователя по статическим образам (сетчатки глаза, отпечаткам пальцев, геометрического вида ладони). Так, для создания биометрического образа с использованием рукописного почерка, пользователю необходимо проделать ряд движение (действий), характерный только ему. Это исключает возможность обмана системы путем предъявления копии (макета) или использования специальных фармакологических препаратов, влияющих на психомоторику человека. Высокая надежность, достаточно быстрые и не требующие специфической технической поддержки алгоритмы и относительно

дешевые приборы ввода данных ставят анализ изменений воспроизведения созданной от руки подписи в ряд наиболее часто применяемых методов аутентификации. Используемые в современном мире устройства для ввода рукописных данных (графические планшеты) в компьютер анализируют не только изменения положения стилуса на плоскости планшета, но и динамику нажатия на него во время письма, что существенно защищает информацию об изменении почерка от чужого вмешательства.

Проведя анализ методов аутентификации статистических и динамических образов пользователей можно сделать следующие выводы.

Биометрическое сканирование статистических образов характеризует точность и практически безотказная работа благодаря не допускающим никаких отклонений алгоритмам распознавания. Благодаря отчетливости использования биометрические методы аутентификации зарекомендовали себя и совершенствуются и дополняются не так часто в связи с тем, что каждый из методов по-своему универсален и возможностей обойти его не так просто.

Биометрическое сканирование динамических образов характеризует объемность и некоторая трудность в работе, из-за гибких алгоритмов распознавания. Благодаря высокой степени защищенности, система может отказать настоящему пользователю в 40 % случаев и имеет некоторые ограничения по использованию. Это происходит из-за того, что не всем пользователям подходит динамическая процедура аутентификации. Подобное исходит из психофизического состояния человека на момент регистрации в системе с последующей идентификацией и аутентификацией в ней.

Методика идентификации с использованием высокоразмерных искусственных нейронных сетей в средствах высоконадежной биометрической аутентификации, способных принимать аутентификационное решение высокой надежности, имеющие в своем составе: биометрические механизмы преобразования биометрических данных в вектора биометрических параметров большой размерности, преобразователи биометрия-код ключа (пароля),

механизмы криптографической аутентификации [13] дает высокую степень защиты данных.

Преимуществами этой методики являются применение размытых (нечетких) динамических биометрических образов – воспроизведение (изображение) голосового (рукописного) пароля (слова, фразы). К достоинствами данной методики можно отнести: высокую непоколебимость средств аутентификации за счет использования нейросетевых преобразователей биометрия-код, легкость ввода и смены пароля (слова, фразы), возможность осуществления автоматической, высоконадежной реальной и удаленной аутентификации обладателя парольного образа, надежное хранение и передача по незащищенным каналам связи биометрических образцов пользователя, дешевизна.

Недостаток этой методики являются большие затраты материальных временных и человеческих ресурсов при сертификации и тестировании данных систем.

Существуют мульти биометрические системы идентификации, использующие несколько биометрических характеристик, что позволяет улучшить защищенность систем контроля доступа.

Биометрические системы контроля доступа удобны для пользователей тем, что носители информации находятся всегда при них, не могут быть утеряны либо украдены. Биометрический контроль доступа считается более надежным, так как идентификаторы не могут быть переданы третьим лицам, скопированы.

Общий принцип работы биометрических систем:

1. Биометрическая система на этапе регистрации и обучения получает образец биометрической особенности пользователя с помощью датчика – например, снимает отпечаток пальца.

2. Из биометрического образца извлекаются индивидуальные параметры – например, минущии (мелкие подробности линий пальца) – с помощью программного алгоритма экстракции черт.

3. Система сохраняет извлеченные параметры в качестве шаблона в базе данных наряду с другими идентификаторами, такими как имя (логин) или идентификационный номер.

4. Пользователь предъявляет датчику еще один биометрический образец. Параметры, извлеченные из него, представляют собой запрос, который система сравнивает с шаблоном заявленной личности с помощью алгоритма сопоставления.

5. Возвращается рейтинг соответствия (мера Хемминга), отражающий степень схожести между шаблоном и запросом. Система принимает заявление, только если рейтинг соответствия превышает заранее заданный порог.

1.3 Обзор средств тестирования биометрической аутентификации

Специфической особенностью биометрической идентификации является большой размер биометрической базы данных: каждый из биометрических образцов должен быть сопоставлен со всеми имеющимися записями в базе данных (сопоставление 1:N или «один ко многим»). Для использования в реальной жизни такая система требует высокой скорости сопоставления биометрических признаков.

Тестирование средств биометрической аутентификации проводится с использованием баз биометрических образов «Свой» и «Чужой», размеры которых являются достаточными для подтверждения характеристик тестируемых средств.

Первоначально средства биометрической идентификации создавались по заказу отдельных лиц и организаций для решения определенных узких задач с небольшим числом идентифицируемых лиц.

Вопрос тестирования с использованием больших баз реальных биометрических образов и об интеграции их или совместимости с другими системами не ставился.

Тестирования средств высоконадежной биометрии достаточно сложная многокритериальная задача [14].

Для определения путей экономии ресурсов при тестировании построена иерархическая структура системы высокоразмерной биометрической аутентификации, представленная на рисунке 1.

Первый этап включает в себя тестирование преобразователя биометрия-код после каждого обучения искусственной нейронной сети (подсистема тестирования преобразователя биометрия-код), в соответствии с требованиями ГОСТ Р 52633.0–2006 [6]. Обучение искусственной нейронной сети должно осуществляться автоматически (без вмешательства человека в процесс подбора параметров искусственной нейронной сети), пользователь должен иметь гарантии того, что его длинный пароль (ключ), участвующий в обучении, не будет скомпрометирован.

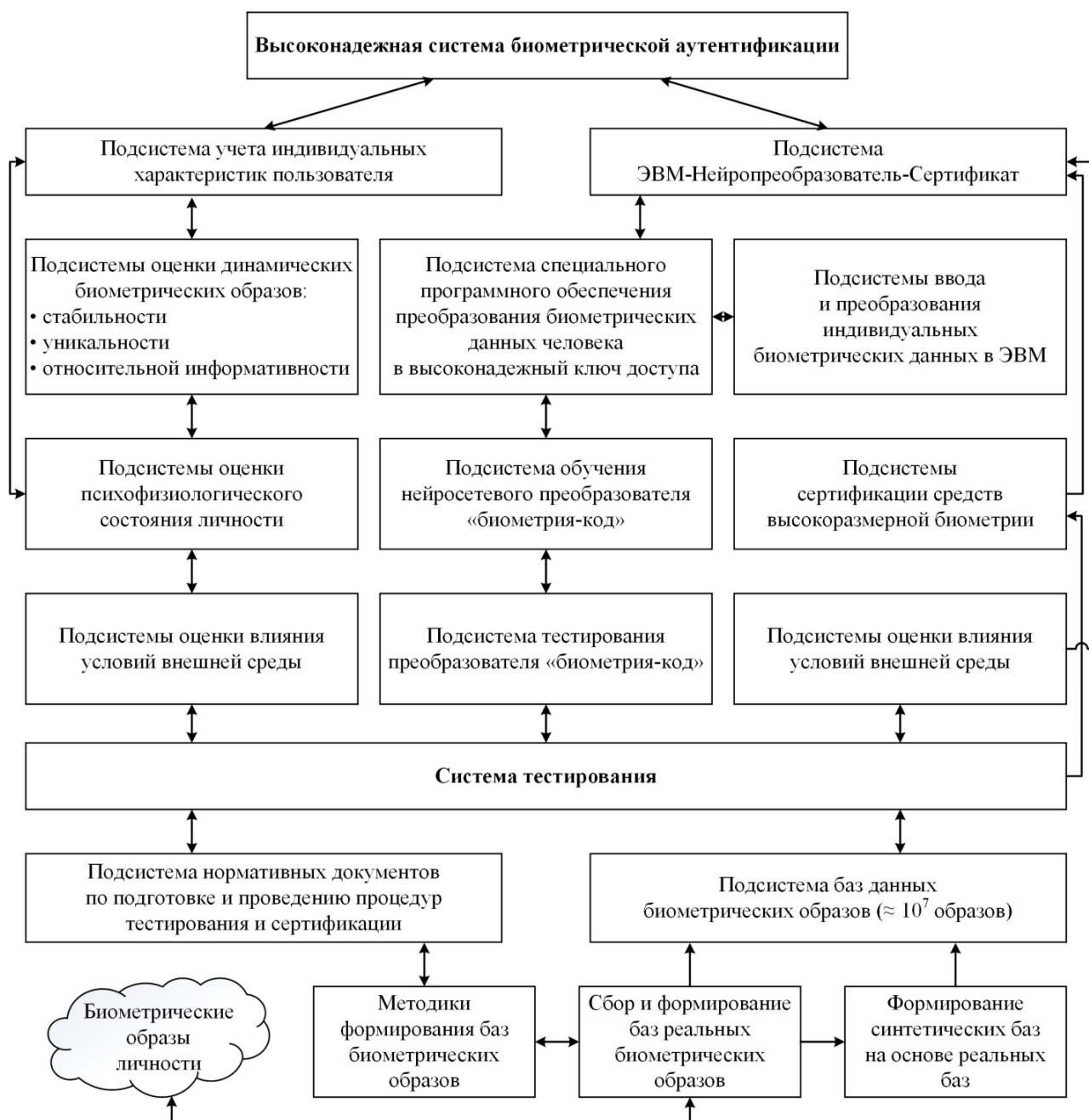


Рисунок 1 – Иерархическая структура системы высоконадежной биометрической аутентификации

При обучении весовые коэффициенты искусственной нейронной сети подбираются автоматом обучения таким образом, чтобы при появлении на входах искусственной нейронной сети элементов вектора «Свой» на выходах нейросети появлялся длинный пароль (ключ). При появлении на входах нейросети векторов данных, соответствующих образам «Чужой», на выходах нейросети должны появляться случайные состояния – «белый шум». Обучение осуществляется путем поочередного предъявления образов «Свой» и «Чужие» с

промежуточным подбором коэффициентов.

Использование существующих алгоритмов, осуществляющих обучение низкоразмерных многослойных искусственных нейронных сетей за десятки часов неприемлемо для высокоразмерных многослойных искусственных нейронных сетей.

Исследования показали, что быстрые алгоритмы позволяют обучать трехслойную искусственную нейронную сеть, преобразующую 416 входных параметра рукописного биометрического слова-пароля из пяти букв в пароль из 32 случайных знаков (ключ длиной 256 бит), за время менее одной минуты. При этом стойкость к атакам подбора рукописного слова-пароля, возрастает с 10^2 до 10^{22} [12].

После обучения системы биометрико-нейросетевой аутентификации необходимо оценить качество обучения. Оцениваются вероятность ошибки первого рода P_1 и вероятность ошибки второго рода P_2 .

Пользователь должен знать реальные оценки стойкости к атакам подбора конкретной реализации биометрической аутентификации после ее обучения, построенной на воспроизведении конкретного тайного биометрического образа. Тестирование осуществляют, используя N_1 -тестовых примера векторов образов «Свой» и N_2 -тестовых примера векторов образов «Чужой». Структурная схема тестирования приведена на рисунке 2 [4].

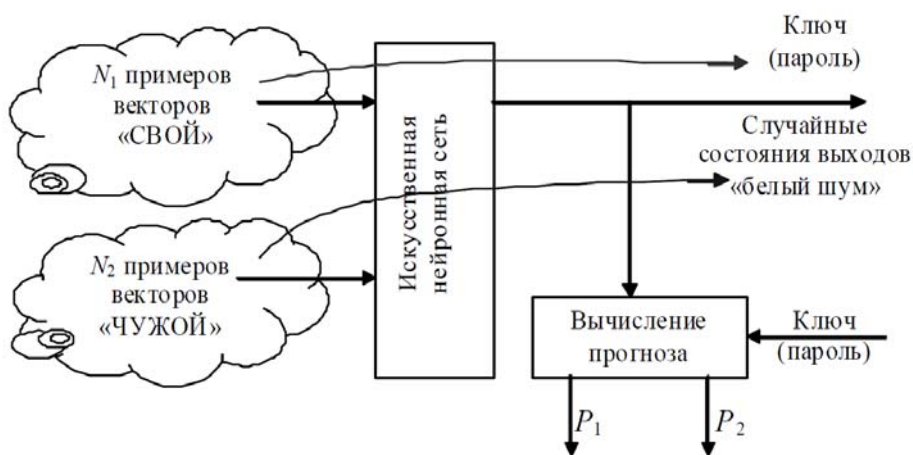


Рисунок 2 – Структурная схема тестирования высокоразмерной системы биометрико-нейросетевой аутентификации после обучения

Следующим этапом стало тестирование самого средства биометрической аутентификации. Цель – подтверждение заявленных производителем характеристик стойкости устройств к атакам подбора ключа.

Для подготовки тестирования в соответствии с ГОСТ Р [6, 15] были созданы и исследованы реальные базы биометрических образов достаточно больших размеров.

Для этого были определены и разработаны требования к представительности реальных биометрических баз рукописных образов; к преобразователям рукописных биометрических образов в электронные образы; к выбору длины рукописного слова-пароля и формированию словаря парольных слов; к программному обеспечению автоматизированного формирования базы рукописных биометрических образов; к условиям формирования базы рукописных биометрических образов; к испытуемым, персоналу и ведению отчетных документов.

Под каждый тип биометрических образов были сформированы свои критерии представительности тестовой выборки.

В качестве критериев представительности были предложены: статистические характеристики среднестатистического пользователя по биометрическому параметру (математическое ожидание, среднеквадратическое отклонение, коэффициенты корреляции); статистические характеристики среднего по некоторой группе пользователей, выделенной по некоторому биометрическому параметру (математическое ожидание, среднеквадратическое отклонение, коэффициенты корреляции); представительность по численности групп пользователей, классифицированных по некоторому биометрическому параметру.

В качестве биометрических параметров были предложены: стабильность, уникальность, стойкость к атакам подбора.

Результаты исследований показали, что пользователи в группах были распределены на 7 классов, один из примеров приведен на рисунке 3 [14].

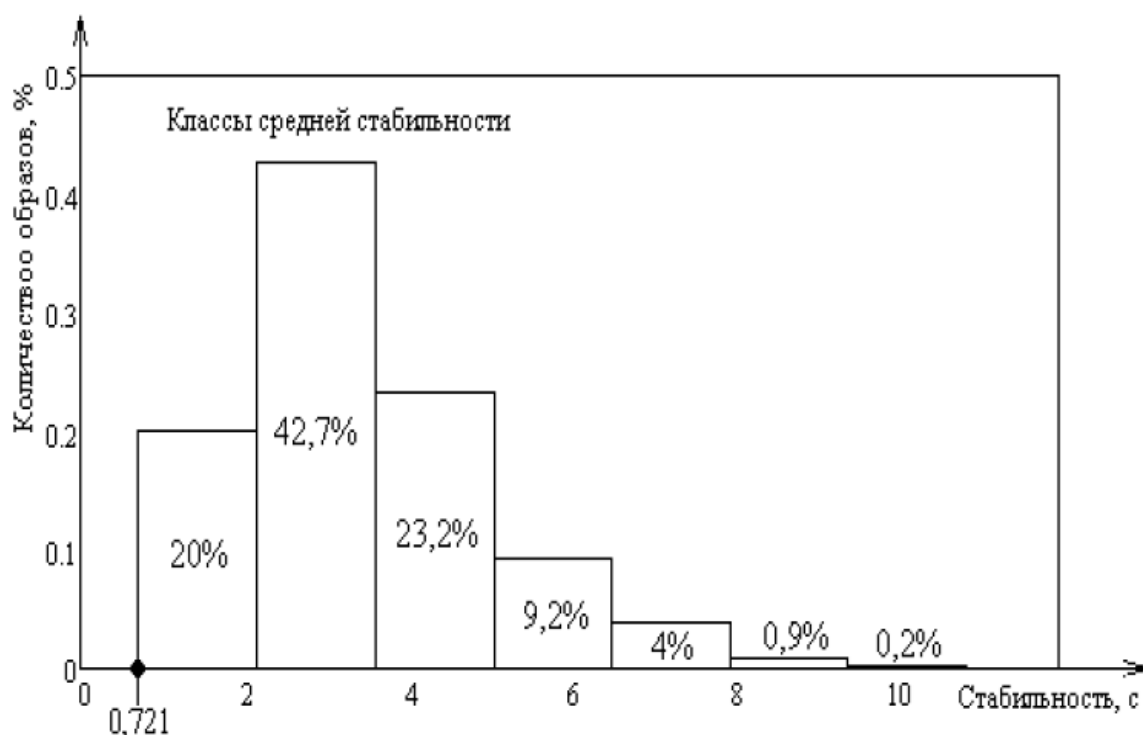


Рисунок 3 – Процентное распределение биометрических рукописных образов «Свой» по классам средней стабильности

Тестирование высоконадежных средств биометрико-нейросетевой аутентификации выполненных в соответствии с ГОСТ Р 52633.0–2006 [6] требует использования от сотен тысяч до миллионов примеров биометрических образов.

В связи с тем, что исследовалось статистическое распределение выходных параметров нейросетевых преобразователей биометрия-код, имеющих значительно большую размерность (порядка 10^9 и выше), то для получения правильного решения количество опытов должно быть увеличено, например до 1500.

Благодаря данному подходу, удастся получить более достоверные результаты тестирования высокоразмерных преобразователей биометрия-код.

1.4 Обзор среды моделирования «БиоНейроАвтограф»

Следует отметить, что задавать корректно биометрические данные достаточно сложно. Если пользоваться некоторым программным генератором данных, то всегда возникает вопрос о том, насколько эти данные корректны. Для того чтобы снять вопрос о корректности получаемых биометрических данных, была создана среда моделирования «БиоНейроАвтограф»; на данный момент это единственный общедоступный инструмент для получения корректных биометрических данных как в русскоязычном сегменте Интернет, так и англоязычном сегменте Интернет.

То, что данные в среде моделирования «БиоНейроАвтограф» корректны, каждый может убедиться самостоятельно, выполнив ряд лабораторных работ, размещенных на сайте АО «ПНИЭИ» <http://пниэи.рф/activity/science/noc.htm>. То, что биометрические данные этого продукта общедоступны, обеспечивается их открытым хранением в директории DATA, среде моделирования «БиоНейроАвтограф», где в процессе работы сохраняются файлы:

- 3sigma.txt (содержит информацию о факте попадания биометрических данных каждого из 416 параметров в его допустимый интервал $\pm 3\sigma$);
- mean.txt (содержит запись среднего значения каждого из 416 контролируемых биометрических параметров);
- mera.txt (содержит меры Хэмминга между кодом «trainKey» и кодом «trainKey», полученные при инициализации режима «проверить»);
- params.txt (содержит 416 биометрических параметров, учитываемых нейронной сетью);
- stdev.txt (содержит 416 стандартных отклонений биометрических параметров, учитываемых нейронной сетью);
- testKeys.txt (содержит данные о коде длиной 256 бит, полученном на выходах нейронной сети при предыдущих проверках);
- trainKey.txt (содержит данные о коде длиной 256 бит, использованном при обучении искусственной нейронной сети);

– weights.txt (содержит данные о 24 весах 256 нейронов преобразователя биометрия-код, полученных в результате последнего обучения).

«БиоНейроАвтограф» – программное обеспечение биометрико-нейросетевой аутентификации пользователей, позволяющее преобразовывать рукописные образы в длинные символьные пароли, и демонстрирующее принцип связывания биометрии пользователя с заданным кодом/паролем.

Предлагаемая программа осуществляет преобразование динамики воспроизведения рукописного слова-пароля в обычный символьный пароль или очень длинный ключ. Слова парольной фразы должны обязательно воспроизводиться рукописным почерком легального пользователя.

В программе используется эмулятор искусственной нейронной сети, имеющей множество выходов. Число выходов искусственной нейронной сети определяется длиной порождаемого ею биометрического ключа. Это исключает взлом программы через обнаружение и подмену последнего бита решающего правила. Программа имеет многобитовое решающее правило, сочетание значений бит которого уникально и злоумышленнику неизвестно.

Преимуществом нейросетевых биометрических хранителей паролей является то, что сам ключ в них не хранится, не хранятся также тайные рукописные биометрические образы. После обучения сети вся эта информация удаляется. Восстановить конфиденциальные данные по структуре связей нейросети и величине ее весовых коэффициентов практически невозможно.

Более того, для каждого пользователя создается уникальный биометрический замок (уникальна и никогда не повторится структура нейросети, генерируемой программой). Это является гарантией того, что опыт, полученный злоумышленниками при взломе имеющегося у них «чужого» замка, будет бесполезен, когда они начнут ломать Ваш личный замок.

2 Оценка вероятности ошибок второго рода и энтропии выходных кодов преобразователя биометрия-код

2.1 Анализ высокоразмерного нейросетевого распознавания образов

Во время обучения нейросетевого преобразователя биометрия-код используются порядка 10 примеров образа «Свой» и в несколько раз больше примеров образов «Чужой». После обучения получается таблица, содержащая номера связей входов 256 нейронов сети с 416 биометрическими параметрами и весовые коэффициенты, каждого нейрона, найденные при обучении.

При распознавании образов происходит преобразование данных, вычисляются биометрические параметры, далее эти параметры передаются на входы искусственной нейронной сети. Обычно искусственная нейронная сеть воспроизводится программно по данным таблицы связей. Процедура распознавания отображена на рисунке 4. Из рисунка видно, что выходной код нейронной сети подается на блок вычисления расстояний Хэмминга. В случае если выходной код нейронной сети точно совпадает с кодом обучения "с" (расстояние Хэмминга нулевое), принимается решение об обнаружении биометрического образа «Свой».

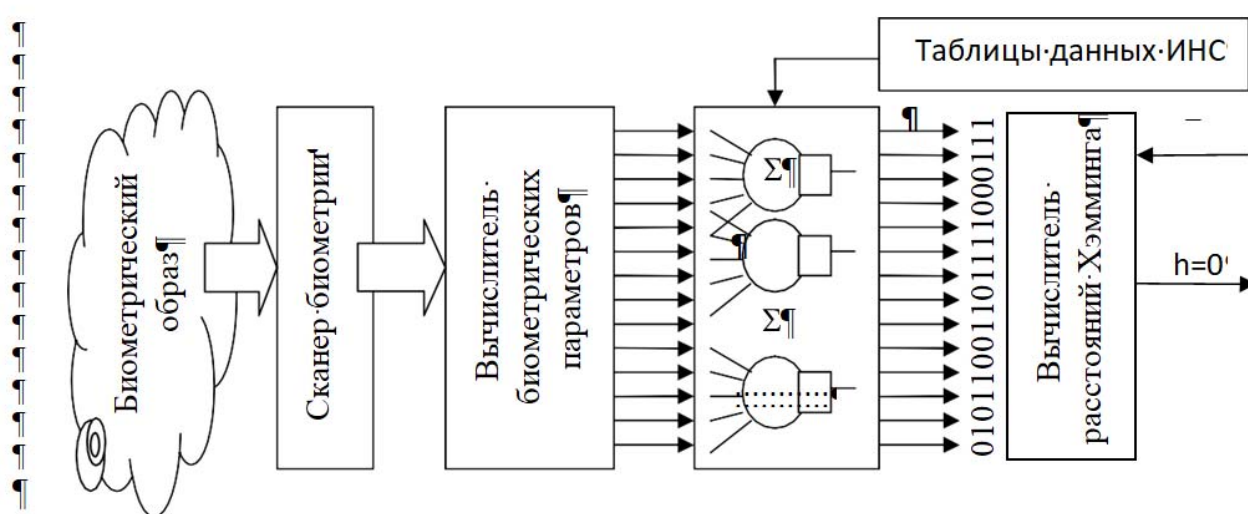


Рисунок 4 – Блок-схема преобразования данных при распознавании образов

Расстояние Хэмминга вычисляется следующим образом:

$$h = \sum_{i=1}^{256} ("c_i") \oplus ("x_i")$$

где $\oplus$ – операция сложения по модулю 2.

Обнаружение нулевого расстояния Хэмминга $h=0$ является идеальным случаем, однако, в предъявленном образе могут быть небольшие отклонения, которые приводят к появлению незначительного числа ошибок $h=1, 2, \dots, h_k$. В пространстве расстояний Хэмминга всегда можно установить порог – h_k принятия решений. При расстояниях Хэмминга менее порога – h_k принимается решение «Свой». Во всех остальных случаях принимается решение «Чужой».

Огромное число алгоритмов обучения нейронных сетей в период второй половины 20 века создавались под сети с одним выходом. В этой постановке задачи различать между собой образы «Чужой-1» и «Чужой-k» нельзя. Их отклики сливаются.

Нейронные сети с большим числом выходов (преобразователи биометрия-код) оказываются много эффективнее нейронных сетей с одним выходом по двум причинам:

- 1) многократно снижены требования к обучению каждого из нейронов;
- 2) стали различимы состояния разных образов «Чужой», что дает дополнительные возможности по исключению коллизий образов «Свой» и все «Чужие».

Важно отметить, что нейронные сети с большим числом выходов в пространстве расстояний Хэмминга ведут себя как квадратичные формы очень высокой размерности. При этом, нейронная сеть размерности 416 входов и 256 выходов имеет абсолютно устойчивый алгоритм быстрого обучения ГОСТ Р 52633.5 [1], тогда как классические квадратичные формы такой размерности настроить технически невозможно.

Совпадение кода на выходе нейросети с кодом аутентификации определяется безопасно некоторым криптографическим протоколам.

2.2 Оценка вероятности ошибок второго рода

Установив некоторый порог допустимых расстояний Хэмминга, мы фактически корректируем в допустимых пределах выходной код нейронной сети. Понятно, что чем больше порог – h_k тем меньше будет вероятность ошибок первого рода – $P_1(h_k)$. Уже при пороге в 5 бит, среда моделирования «БиоНейроАвтограф» практически перестает ошибаться. Однако, при этом вероятность ошибок второго рода – $P_2(h_k)$ увеличивается. В связи с этим очень важно уметь вычислять эту вероятность. Для оценки необходимо подать на входы нейронной сети несколько десятков примеров образов все «Чужие». Схема численного эксперимента приведена на рисунке 5.

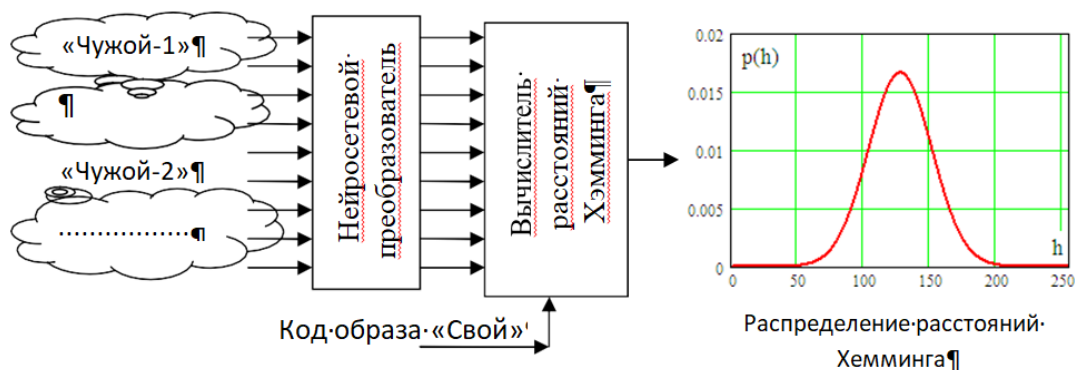


Рисунок 5 – Оценка вероятности ошибок второго рода, обученного нейросетевого преобразователя

При этом эксперименте мы получаем выборку расстояний Хэмминга $\{h_1, h_2, h_3, \dots, h_{32}\}$. Эта выборка позволяет вычислить их математическое ожидание – $E(h)$ и стандартное отклонение – $\sigma(h)$. Располагая этими данными, мы можем воспользоваться рекомендациями ГОСТ Р 52633.3 [9] и определить вероятность ошибок второго рода по следующей формуле:

$$P_2(h_k) \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{h_k} \exp\left\{-\frac{(E(h)-u)^2}{2(\sigma(h))^2}\right\} \cdot du$$

Многомерная энтропия выходных кодов нейросетевого преобразователя оценивается через вероятность ошибок второго рода:

$$H("x_1, x_2, ..., x_{256}") \approx -\log_2(P_2(h_k))$$

2.3 Тестирование в среде моделирования «БиоНейроАвтограф»

Как говорилось выше – среда моделирования «БиоНейроАвтограф» предназначена для нейросетевого связывания рукописного пароля с обычным паролем доступа (набираемым на клавиатуре) или криптографическим ключом.

В данной системе аутентификации один из вариантов автоматизированного тестирования: тестирование на тестовых образах, который представляет собой тестирование на реальных рукописных образах из базы тестовых примеров. Данный вид тестирования позволяет оценить стойкость системы биометрической аутентификации при атаках с помощью больших баз биометрических примеров. Моделируется ситуация когда злоумышленник, располагающий базой образов, пытается взломать вашу защиту.

Для того, чтобы обучить нейронную сеть, необходимо ввести несколько обучающих примеров рукописных образов/паролей «Пенза» пользователя «Свой». При обучении системы, необходимо передать системе данные образы.

Результат создания девяти образов «Свой» представлен на рисунке 6.

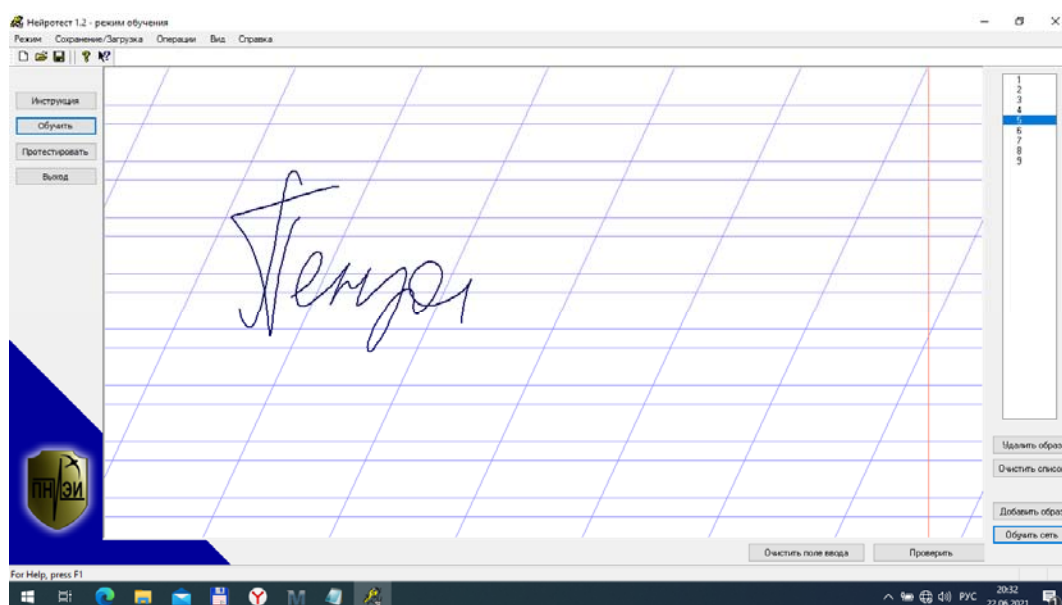


Рисунок 6 – Просмотр рукописных образов перед обучением

После добавления в список обучающих примеров рукописного образа запускается процесс обучения нейронной сети, выполнив команду «Обучить сеть». Обучение сети из 256 нейронов длится менее 1 с. По окончании обучения появляется окно с результатами обучения, содержащее информацию о предполагаемой стабильности введенных биометрических примеров, вероятности узнавания образа «Свой» и ожидаемой стойкости системы к атакам подбора обучающего рукописного слова-пароля, т.е. вероятность пропуска образа «Чужой» (рисунок 7)

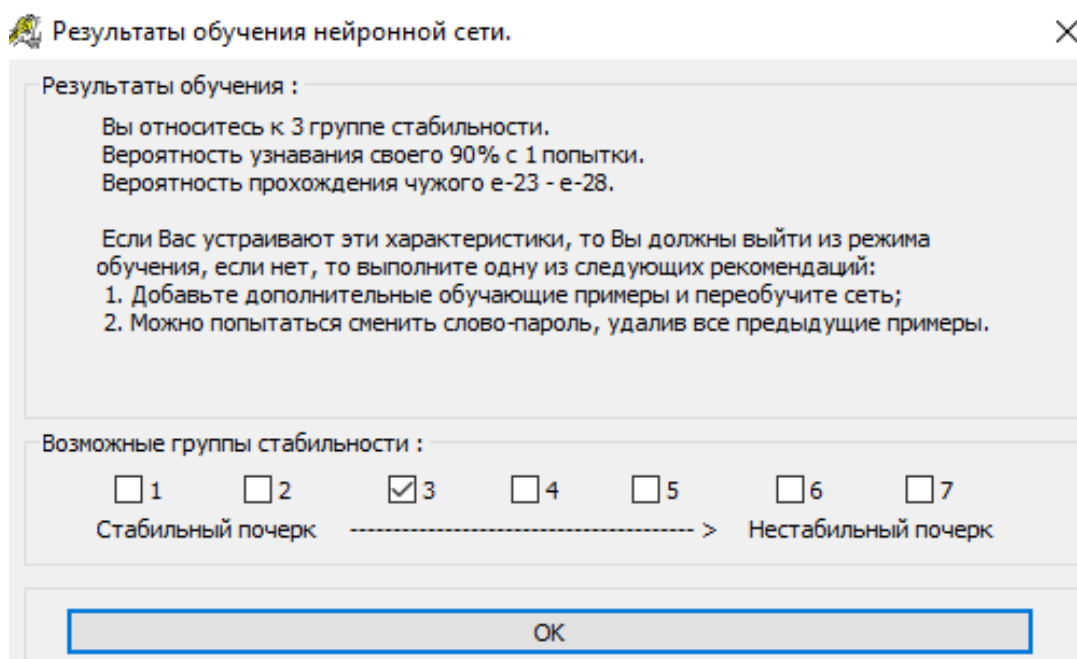


Рисунок 7 – Окно результатов обучения

Программа сообщает группу стабильности пользователя на выбранном рукописном пароле и вероятность возникновения ошибок первого рода (принимает «Свой» за «Чужой») и второго рода (принимает «Чужой» за «Свой»).

Доверие к результатам обучения, отображаемым в окне с результатами обучения, выше среднего – вероятность узнавания «Свой» – 90 %, а вероятность прохождения «Чужой» низкая.

Можно попытаться изменить качество обучения, увеличивая или уменьшая число примеров обучения. Более точную оценку качества обучения можно дать только после тестирования искусственной нейронной сети.

Для того чтобы получить достоверную оценку качества обучения, необходимо в поле ввода рукописных образов ввести пример рукописного образа «Свой» и нажать кнопку «Проверить» и система выдаст сообщение о том, распознан введенный образ системой как «Свой» или нет.

При этом вычисляются параметры введенного рукописного образа, они подаются на входы искусственной нейронной сети, вычисляется выходной код и выводится окно, в котором показывается сгенерированный нейросетью ключ в двоичной кодировке (10100110-...) и символьном представлении (e9c7uJvv...) с результатами сравнения полученного выходного кода с обучающим кодом (рисунок 8).

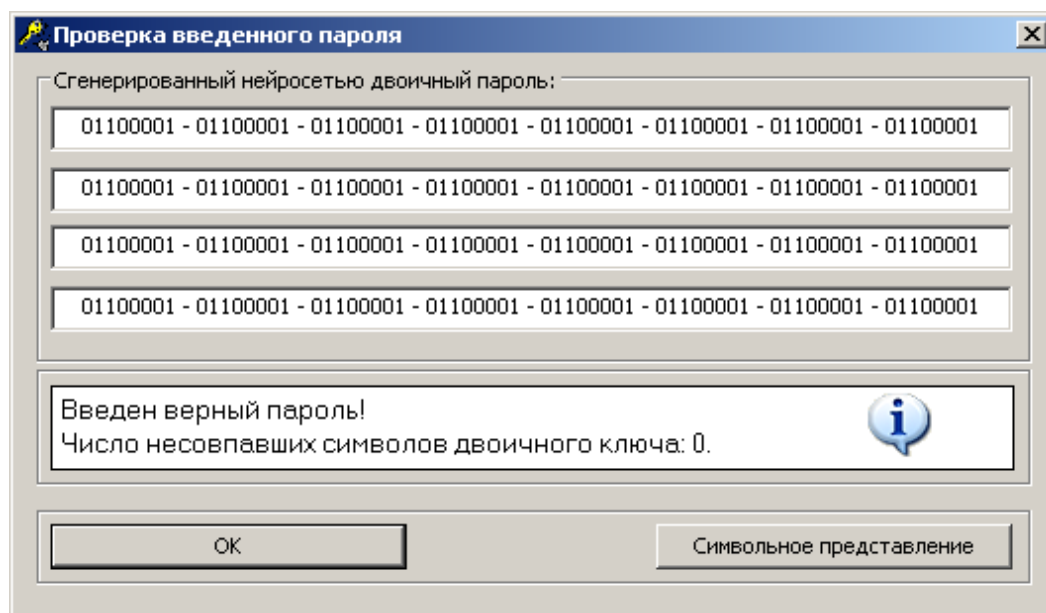


Рисунок 8 – Ввод образа «Свой»

Сеть хорошо узнает образ «Свой», если мера Хэмминга на тестовых примерах равна нулю (все разряды полученного кода совпадают с заданным при обучении кодом «Свой»).

Для проверки способности нейронной сети отказывать в доступе образам «Чужой» необходимо воспроизвести случайное рукописное слово (букву). При этом появляется случайный код, совпадающий с кодом «Свой» в случайных разрядах. В окне вывода полученного кода совпавшие разряды отображаются верными состояниями "0" и "1", а не совпавшие разряды отображаются символом "*".

В случае ввода неправильного рукописного образа (рисунок 9) появляется окно, изображённое на рисунке 10. Звёздочками помечаются не совпавшие биты исходного ключа и сгенерированного. Также отображается общее количество не совпавших символов двоичного ключа.

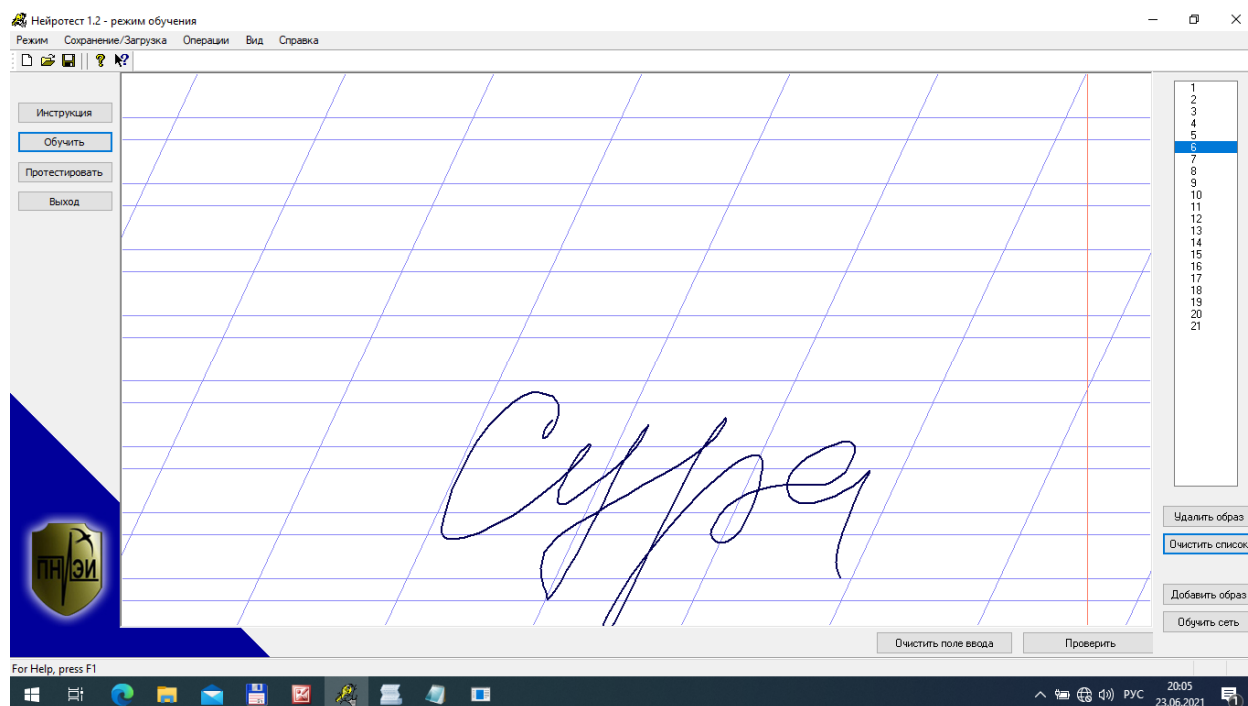


Рисунок 9 – Ввод образа «Чужой»

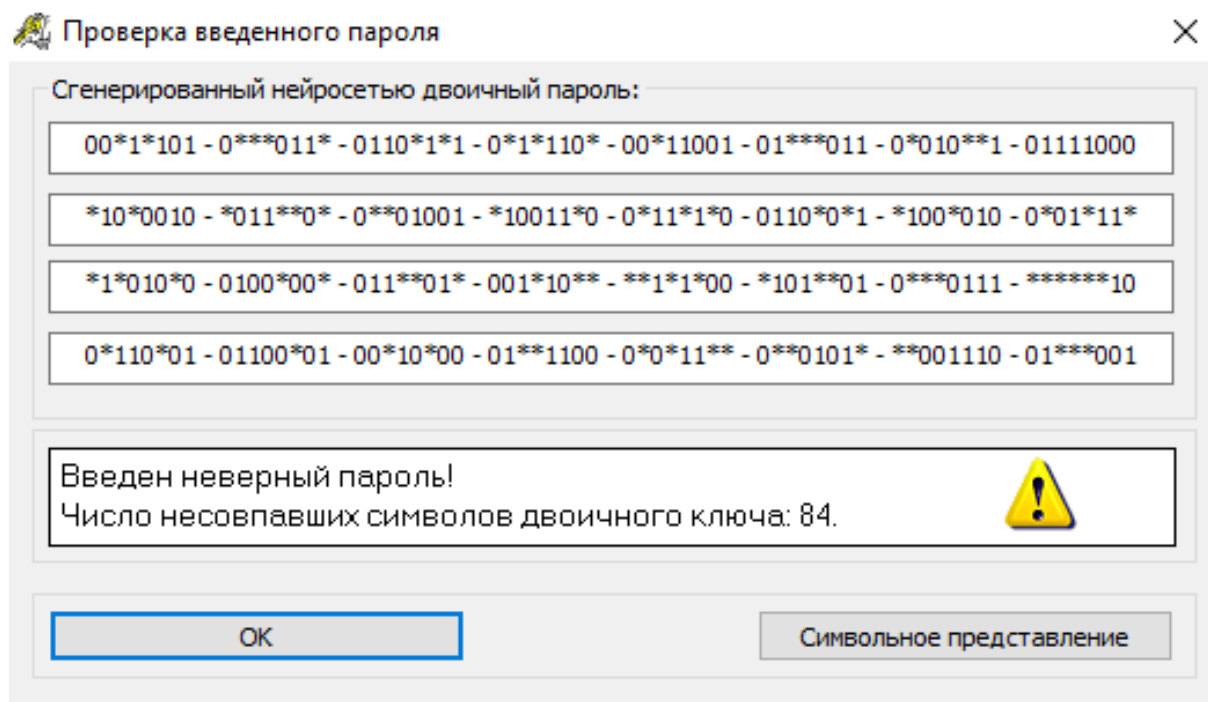


Рисунок 10 – Проверка ввода образа «Чужой»

При подготовке к тестированию была создана база тестовых образов «Сура21», состоящая из 21 образа «Чужой» (рисунок 9). Для запуска процедуры тестирования на тестовых образах следует выбрать пункт меню «Операции» «Тестировать на тестовых образах» (рисунок 11).

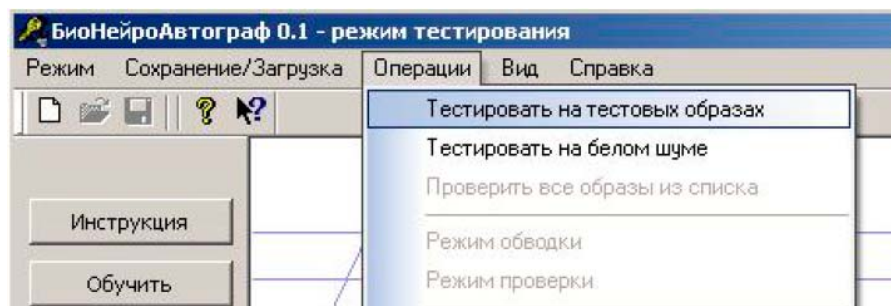


Рисунок 11 – Запуск тестирования на реальных образах

Затем указать базу тестовых образов, и запустится механизм оценки стойкости к атакам подбора. На рисунке 12 представлен полученный результат тестирования.

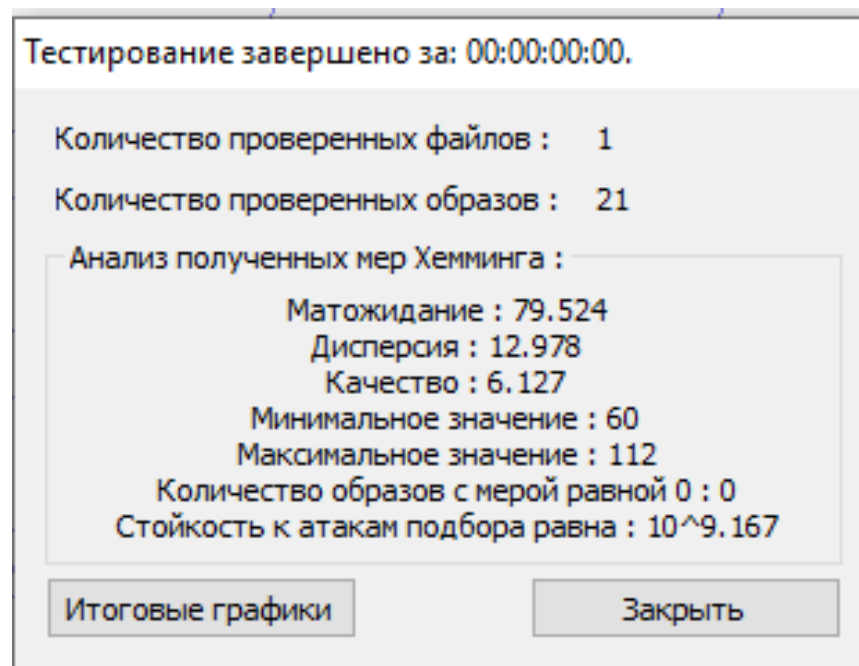


Рисунок 12 – Результат тестирования на тестовых образах

Все вычисляемые во время тестирования меры Хемминга записываются в файл Data/<Имя_пользователя>/mera.txt. Каталог Data находится рядом с запускаемым файлом БиоНейроАвтограф.exe. После каждого тестирования происходит перезаписывание данных в файле mera.txt.

Из рисунка 12 видно, что окно результатов содержит информацию о количестве использовавшихся во время тестирования примеров реальных рукописных образов – 21, математическое ожидание – 79,524, среднеквадратическое отклонение 12,978, качество, минимальное и максимальное значение полученных мер Хемминга – 60 и 112 соответственно. Также отображается количество «взломов» системы (количество образов с нулевой мерой) и вычисленная на тестовой базе стойкость к атакам подбора – $10^{9,2}$.

Получаем ошибку второго рода $P_2=10^{-92}$. То есть «Чужой» образ «Сура» с 10^9 попытки совпадет с образом «Свой» «Пенза», из чего следует, что качество защиты – высокое.

3 Оценка корреляционной сцепленности кодов откликов внутри двух групп образов «Чужой»

3.1 Оценка коррелированности выходного состояния преобразователей биометрия-код

Для биометрии актуальна тематика запутанности единиц информации (бит). В работе [1] было показано, что реальная энтропия 256 выходного кода нейронной сети оказывается меньше. Наблюдается дефект энтропии, обусловленный наличием корреляционных связей между случайными состояниями разрядов. Чем больше корреляция между разрядами кодов, тем меньше энтропия кодов. Оценить корреляцию между разрядами кодов удастся через вычисления следующего функционала:

$$R(q) = \left(1 - \frac{H("x_1, x_2, \dots, x_q")}{q} \right)$$

В случае если $q=256$ разрядов выходных кодов нейронной сети являются белым шумом, то их совместная энтропия составит 256 бит. Корреляционный функционал в этом случае оказывается нулевым $R(256)=0$. В противоположной ситуации, когда на вход нейронной сети подаются примеры данных образа «Свой», выходная энтропия кодов оказывается нулевой. Как результат, функционал принимает единичное значение $R(256)=1$.

Энтропия реальных рукописных образов среды «БиоНейроАвтограф» находится в интервале от 0 бит до 58 бит для самых стабильных и самых уникальных образов рукописного пароля. Это означает, что корреляционный функционал может измениться в интервале от 1 до 0.733.

3.2 Численный эксперимент оценки коррелированности ключей образов «Чужой»

Опишем численный эксперимент оценки коррелированности ключей образов «Чужой».

Среда моделирования «БиоНейроАвтограф» не может читать длинные строки в 256 бит кода, из файла «TextKeyХопер.txt».

Файл «TextKeyХопер.txt» получается в результате загрузки заранее сгенерированных 21 примера образа «Чужой» «Хопер». При тестирование инициированном командой «Проверить» среда моделирования «БиоНейроАвтограф» записывает результаты выходных кодов в файл «TestKeys txt». Результат представлен на рисунке 13.



Рисунок 13 – Запись результатов выходных кодов в файл «TestKeys txt»

На рисунке отображены ключи в 8-битном, 16-битном и 256-битном исполнении. Для расчета коэффициентов корреляции необходим только 256-битный ключ. Для этого нужно открыть файл любым редактором, например встроенным в TotalComander и отредактировать длинную строчку в 256 символов (рисунок 14), в вектор для MathCad (рисунок 15).

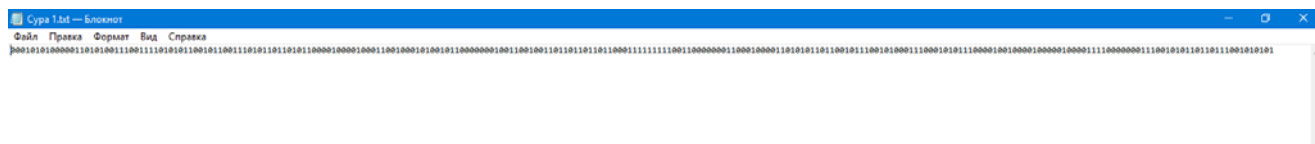


Рисунок 14 – Отображение 256-битного ключа
перед редактированием

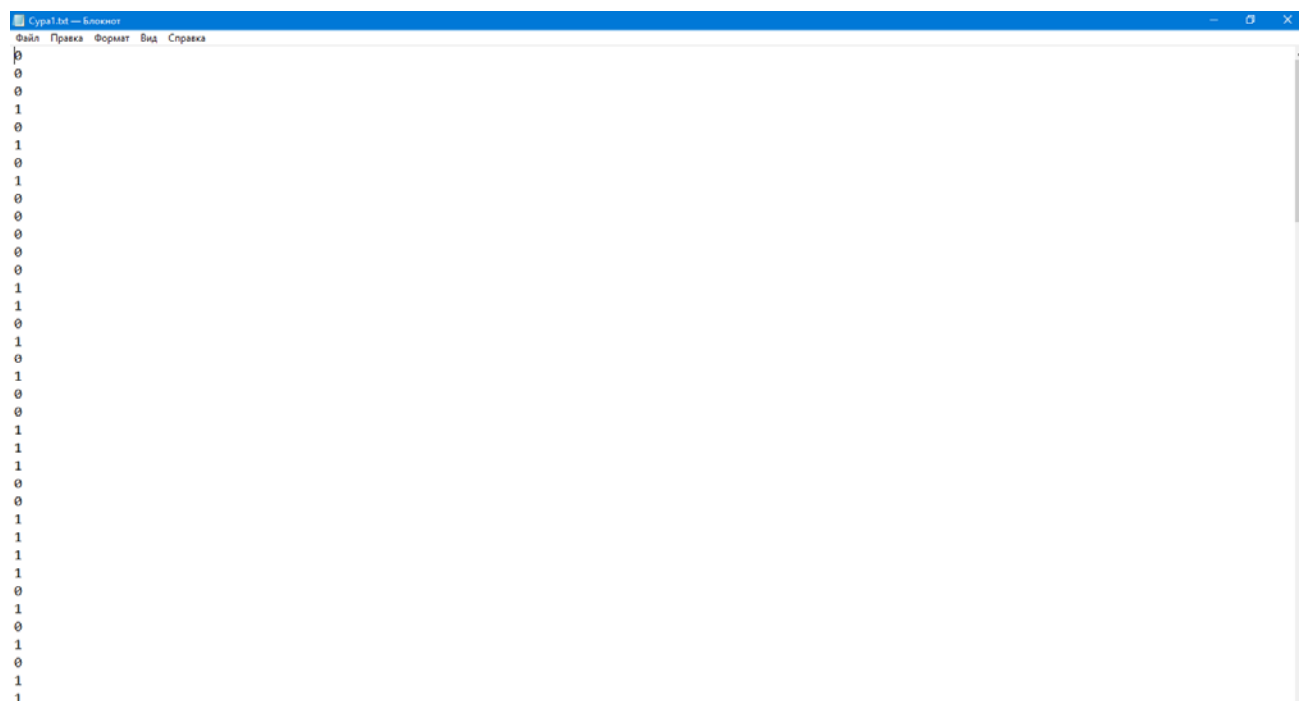


Рисунок 15 – Отображение 256-битного ключа
после редактирования

Операцию повторить для каждого образа «Хонер» и для каждого образа «Сура» и сохранить каждый в отдельный файл формата *.txt. Результат представлен на рисунках 16 и 17.

 Сура1	23.06.2021 1:32	Текстовый докум...	1 КБ
 Сура2	23.06.2021 1:33	Текстовый докум...	1 КБ
 Сура3	23.06.2021 1:34	Текстовый докум...	1 КБ
 Сура4	23.06.2021 1:35	Текстовый докум...	1 КБ
 Сура5	23.06.2021 1:36	Текстовый докум...	1 КБ
 Сура6	23.06.2021 1:39	Текстовый докум...	1 КБ
 Сура7	23.06.2021 1:40	Текстовый докум...	1 КБ
 Сура8	23.06.2021 1:42	Текстовый докум...	1 КБ
 Сура9	23.06.2021 1:43	Текстовый докум...	1 КБ
 Сура10	23.06.2021 1:43	Текстовый докум...	1 КБ
 Сура11	23.06.2021 1:44	Текстовый докум...	1 КБ
 Сура12	23.06.2021 1:45	Текстовый докум...	1 КБ
 Сура13	23.06.2021 1:46	Текстовый докум...	1 КБ
 Сура14	23.06.2021 1:46	Текстовый докум...	1 КБ
 Сура15	23.06.2021 1:47	Текстовый докум...	1 КБ
 Сура16	23.06.2021 1:48	Текстовый докум...	1 КБ
 Сура17	23.06.2021 1:49	Текстовый докум...	1 КБ
 Сура18	23.06.2021 1:50	Текстовый докум...	1 КБ
 Сура19	23.06.2021 1:52	Текстовый докум...	1 КБ
 Сура20	23.06.2021 1:52	Текстовый докум...	1 КБ
 Сура21	09.06.2017 9:02	Файл "DAT"	70 КБ
 Сура21	23.06.2021 1:53	Текстовый докум...	1 КБ

Рисунок 16 – Отредактированные данные базы «Сура»

 Хопер0	09.06.2021 9:17	Текстовый докум...	1 КБ
 Хопер1	09.06.2021 9:27	Текстовый докум...	1 КБ
 Хопер2	09.06.2021 9:43	Текстовый докум...	1 КБ
 Хопер3	23.06.2021 1:21	Текстовый докум...	1 КБ
 Хопер4	22.06.2021 21:39	Текстовый докум...	1 КБ
 Хопер5	22.06.2021 20:42	Текстовый докум...	1 КБ
 Хопер6	22.06.2021 21:45	Текстовый докум...	1 КБ
 Хопер7	22.06.2021 21:49	Текстовый докум...	1 КБ
 Хопер8	22.06.2021 21:51	Текстовый докум...	1 КБ
 Хопер9	22.06.2021 21:53	Текстовый докум...	1 КБ
 Хопер10	22.06.2021 21:56	Текстовый докум...	1 КБ
 Хопер11	22.06.2021 21:59	Текстовый докум...	1 КБ
 Хопер12	23.06.2021 0:58	Текстовый докум...	1 КБ
 Хопер13	23.06.2021 0:57	Текстовый докум...	1 КБ
 Хопер14	23.06.2021 0:56	Текстовый докум...	1 КБ
 Хопер15	23.06.2021 0:55	Текстовый докум...	1 КБ
 Хопер16	23.06.2021 0:54	Текстовый докум...	1 КБ
 Хопер17	23.06.2021 0:53	Текстовый докум...	1 КБ
 Хопер18	23.06.2021 0:52	Текстовый докум...	1 КБ
 Хопер19	23.06.2021 0:51	Текстовый докум...	1 КБ
 Хопер20	23.06.2021 0:50	Текстовый докум...	1 КБ

Рисунок 17 – Отредактированные данные базы «Хопер»

Далее нужно посчитать математическое ожидание расстояния коэффициентов корреляции и стандартное отклонение коэффициентов корреляции.

Для этого в MathCad вводим все отредактированные образы Хопер и с помощью команды «READPRN» присваиваем каждому ключу переменную «х». Результат представлен на рисунках 18 и 19.

```

x1 := READPRN("Хопер1.txt")    x12 := READPRN("Хопер12.txt")
x2 := READPRN("Хопер2.txt")    x13 := READPRN("Хопер13.txt")
x3 := READPRN("Хопер3.txt")    x14 := READPRN("Хопер14.txt")
x4 := READPRN("Хопер4.txt")    x15 := READPRN("Хопер15.txt")
x5 := READPRN("Хопер5.txt")    x16 := READPRN("Хопер16.txt")
x6 := READPRN("Хопер6.txt")    x17 := READPRN("Хопер17.txt")
x7 := READPRN("Хопер7.txt")    x18 := READPRN("Хопер18.txt")
x8 := READPRN("Хопер0.txt")    x19 := READPRN("Хопер19.txt")
x9 := READPRN("Хопер9.txt")    x20 := READPRN("Хопер20.txt")
x10 := READPRN("Хопер10.txt")  x21 := READPRN("Хопер21.txt")
x11 := READPRN("Хопер11.txt")

```

Рисунок 18 – Присвоение каждому образу значение «х»

$$x_0^T =$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	1	1	1	...

Рисунок 19 – Пример отображения части 256-и битного кода

Вычисляем коэффициент корреляции между двумя векторами, с помощью функции «corr». Результат представлен на рисунке 20.

```

R01 := corr(x0,x1)    corr(x0,x1) = 0.371
R02 := corr(x0,x2)

R03 := corr(x0,x3)
R04 := corr(x0,x4)
R05 := corr(x0,x5)
R06 := corr(x0,x6)
R07 := corr(x0,x7)
R08 := corr(x0,x8)
R09 := corr(x0,x9)
R010 := corr(x0,x10)
R011 := corr(x0,x11)
R012 := corr(x0,x12)
R013 := corr(x0,x13)

R014 := corr(x0,x14)
R015 := corr(x0,x15)
R016 := corr(x0,x16)
R017 := corr(x0,x17)
R018 := corr(x0,x18)
R019 := corr(x0,x19)
R020 := corr(x0,x20)

R12 := corr(x1,x2)
R13 := corr(x1,x3)
R14 := corr(x1,x4)
R15 := corr(x1,x5)
R16 := corr(x1,x6)
R17 := corr(x1,x7)

```

Рисунок 20 – Расчет коэффициента корреляции

Далее считаем математическое ожидание с помощью функции «mean». Результат представлен на рисунке 21.

```

m1 := mean(R01,R02,R03,R04,R05,R06,R07,R08,R09,R010)
m1 = 0.431

m2 := mean(R011,R012,R013,R014,R015,R016,R017,R018,R019,R020)
m2 = 0.382

m3 := mean(R12,R13,R14,R15,R16,R17,R18,R19,R23,R24)
m3 = 0.484

M := mean(m1,m2,m3)
M = 0.432

```

Рисунок 21 – Расчет математического ожидания

Далее считаем стандартное отклонение с помощью функции «stdev». Результат представлен на рисунке 22.

$$s1 := \text{stdev}(R01, R02, R03, R04, R05, R06, R07, R08, R09, R010) \quad s1 = 0.224$$

$$s2 := \text{stdev}(R011, R012, R013, R014, R015, R016, R017, R018, R019, R020) \quad s2 = 0.079$$

$$s3 := \text{stdev}(R12, R13, R14, R15, R16, R17, R18, R19, R23, R24) \quad s3 = 0.085$$

$$SS := \text{mean}(s1, s2, s3) \quad SS = 0.129$$

Рисунок 22 – Расчет стандартного отклонения.

С помощью построения графиков в MathCad интерпретируем результаты численного эксперимента в график. Результат представлен на рисунке 23.

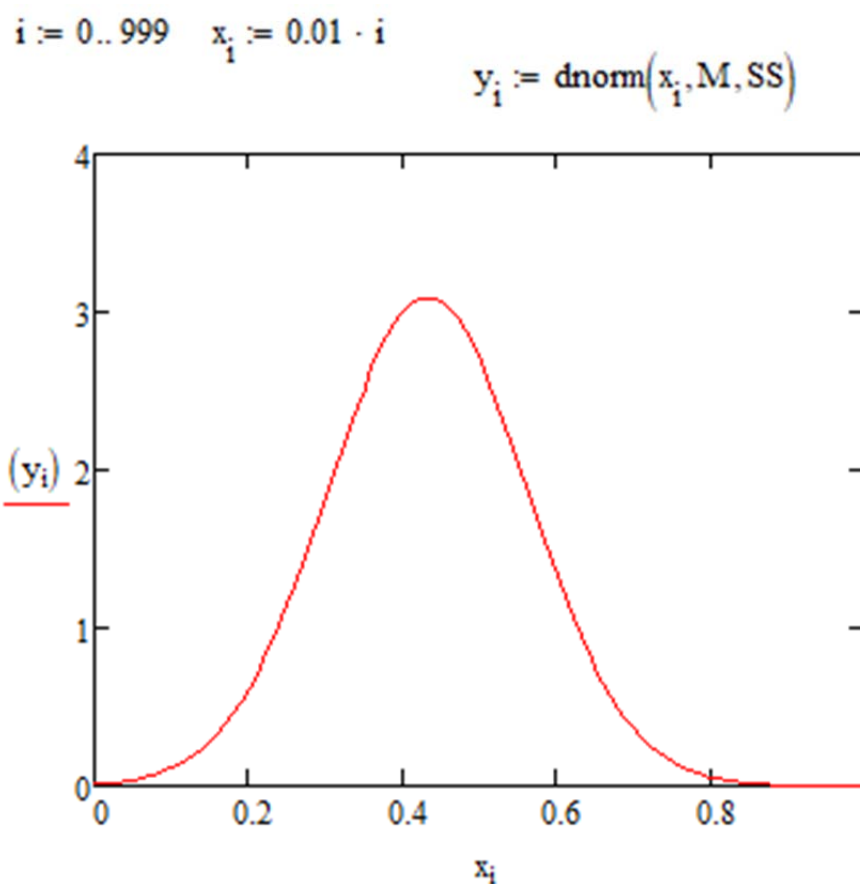


Рисунок 23 – Распределение расстояний корреляционной сцепленности между ключами от примеров образов «Хонер»

Повторяем те же операции с заранее подготовленными образами «Сура»:

- присвоение каждому образу значение «х»;
- вычисление коэффициента корреляции между двумя векторами;
- вычисление математического ожидания;
- вычисление стандартного отклонения;
- интерпретация результатов численного эксперимента в график.

Результат приведен на рисунке 24 и в приложении Б.

$$i := 0..999 \quad x_i := 0.01 \cdot i \quad y_i := \text{dnorm}(x_i, M, SS)$$

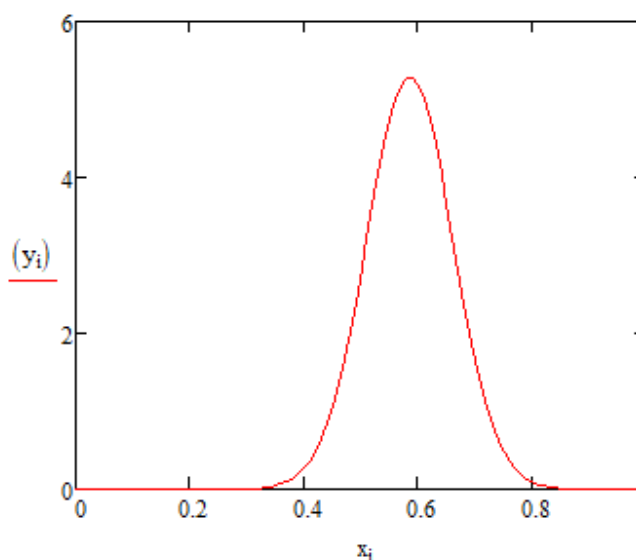


Рисунок 24 – Распределение расстояний корреляционной сцепленности между ключами от примеров образов «Сура»

Из приведенных расчетов и их анализа видно, что прямое вычисление коэффициентов корреляции («corr» (x0, x1....)) позволяет определить корреляционную сцепленность кодов образов «Чужой» («Хонер», «Сура»). Этой функцией необходимо расширить среду моделирования «БиоНейроАвтограф».

4 Подтверждение результатов численного моделирования через меру Хемминга (методика Ратникова)

Оценка коррелированности выходных состояний преобразователей биометрия-код были освещены в 2016 г. [1]

Энтропия реальных рукописных образов всегда намного меньше, чем идеальная белого шума в 256 бит. Разряды кодов нейронной сети всегда оказываются значительно коррелированы. Связь корреляционных функционалов (1) со средним модулем обычных коэффициентов корреляции $E\{|r|\}$ [17, 18] приведена на номограмме рисунка 25.

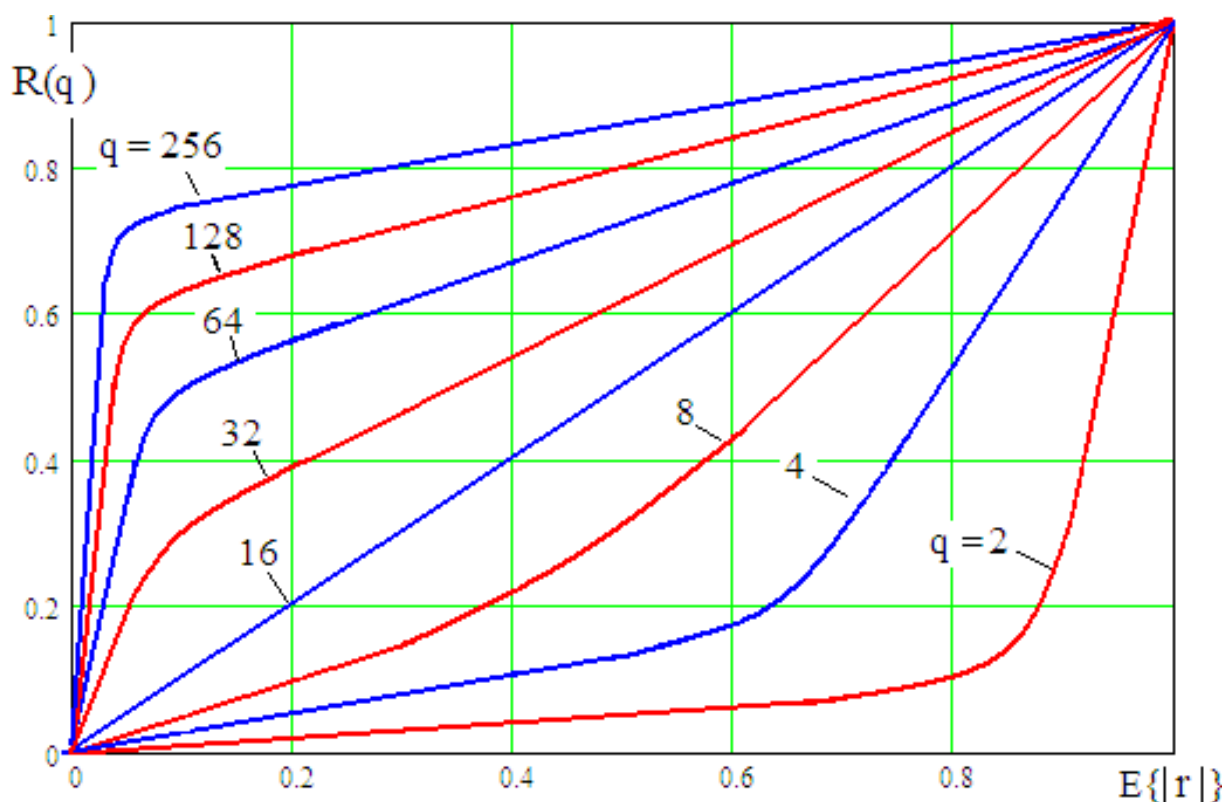


Рисунок 25 – Номограмма связи корреляционных функционалов $R(q)$ со значением среднего значения модулей обычных коэффициентов корреляции

Из рисунка 25 видно, что размерность $q=16$ является прямой линией. То есть, проще всего оценивать энтропию биометрических данных используя 16-ти битные фрагменты кодов. Вычислив многократно среднее значение модулей парных корреляционных связей, мы можем найти $R(q=16)$ и далее, пользуясь

номограммой рисунка 25 для определения $R(q=256)$. В свою очередь, по значению $R(q=256)$ мы можем восстановить значение 256 мерной энтропии.

Так же из рисунка 25 видно, что размерность $q=16$ играет особую пограничную роль между низкоразмерными и высокоразмерными системами. Кривые связи низкоразмерной энтропии и высокоразмерной энтропии со средним модулем обычной корреляции имеют противоположную выпуклость. Они приближаются разными уравнениями в интервале числа выходов от 2 до 16 и в интервале числа выходов от 16 до 256.

4.1 Численный эксперимент оценки коррелированности ключей образов «Чужой» с использованием функции «Сумма значений переменной диапазона»

В 2020 аспирантом Ратниковым [16] была предложена более простая процедура вычисления корреляционной сцепленности через расчет математических ожиданий расстояния Хемминга между сравниваемыми кодами. Эта методика позволяет повторить те же самые вычисления для образов «Сура» и «Хопер», выполнить их в среде моделирования MathCad. Результатом ожидается если не полное совпадение коэффициентов, то максимально приближенное.

Для вычисления математического ожидания и стандартного отклонения Хемминга потребуются заранее заготовленные отредактированные группы образов «Чужой» «Хопер» (Рисунок 17), которые использовались для расчетов в п. 3 ВКР, а также данные базы ключей с присвоенной переменной «х» из среды математического моделирования MathCad (Рисунок 18).

Далее вычисляем коэффициент корреляции между двумя векторами с помощью функции «Сумма значений переменной диапазона». Результат представлен на рисунке 26.

$$\begin{aligned}
R01 &:= \sum_{i=0}^{255} (x0_i \oplus x1_i) & R02 &:= \sum_{i=0}^{255} (x0_i \oplus x2_i) & R03 &:= \sum_{i=0}^{255} (x0_i \oplus x3_i) \\
R04 &:= \sum_{i=0}^{255} (x0_i \oplus x4_i) & R05 &:= \sum_{i=0}^{255} (x0_i \oplus x5_i) & R06 &:= \sum_{i=0}^{255} (x0_i \oplus x6_i) \\
R07 &:= \sum_{i=0}^{255} (x0_i \oplus x7_i) & R08 &:= \sum_{i=0}^{255} (x0_i \oplus x8_i) & R09 &:= \sum_{i=0}^{255} (x0_i \oplus x9_i) \\
R010 &:= \sum_{i=0}^{255} (x0_i \oplus x10_i) & R011 &:= \sum_{i=0}^{255} (x0_i \oplus x11_i) & R012 &:= \sum_{i=0}^{255} (x0_i \oplus x12_i) \\
R013 &:= \sum_{i=0}^{255} (x0_i \oplus x13_i) & R014 &:= \sum_{i=0}^{255} (x0_i \oplus x14_i) & R015 &:= \sum_{i=0}^{255} (x0_i \oplus x15_i) \\
R016 &:= \sum_{i=0}^{255} (x0_i \oplus x16_i) & R017 &:= \sum_{i=0}^{255} (x0_i \oplus x17_i) & R018 &:= \sum_{i=0}^{255} (x0_i \oplus x18_i) \\
R019 &:= \sum_{i=0}^{255} (x0_i \oplus x19_i) & R020 &:= \sum_{i=0}^{255} (x0_i \oplus x20_i) & R12 &:= \sum_{i=0}^{255} (x1_i \oplus x2_i) \\
R13 &:= \sum_{i=0}^{255} (x1_i \oplus x3_i) & R14 &:= \sum_{i=0}^{255} (x1_i \oplus x4_i) & R15 &:= \sum_{i=0}^{255} (x1_i \oplus x5_i) \\
R16 &:= \sum_{i=0}^{255} (x1_i \oplus x6_i) & R17 &:= \sum_{i=0}^{255} (x1_i \oplus x7_i) & &
\end{aligned}$$

Рисунок 26 – Вычисление коэффициента корреляции между двумя векторами помощью функции «Сумма значений переменной диапазона»

Переходим к вычислениям математического ожидания и стабильного отклонения с помощью тех же функций, что и в п. 3 для получения материала для сравнения.

Вычисляем математическое ожидание расстояния Хемминга с помощью функции «mean». Результат представлен на рисунке 27.

Вычисляем стабильное отклонение расстояния Хемминга с помощью функции «stdev». Результат представлен на рисунке 28.

Вычисление Мат. Ожиданий.

```
m1 := mean(R01,R02,R03,R04,R05,R06,R07,R08,R09,R010)
m1 = 72.8

m2 := mean(R011,R012,R013,R014,R015,R016,R017,R018,R019,R020)
m2 = 79.3

m3 := mean(R12,R13,R14,R15,R16,R17,R18,R19,R23,R24)
m3 = 39.389

M := mean(m1,m2,m3)
M = 63.83
```

Рисунок 27 – Вычисление математического ожидания
расстояния Хемминга

Вычисление стандартного отклонения

```
s1 := stdev(R01,R02,R03,R04,R05,R06,R07,R08,R09,R010)
s1 = 28.701

s2 := stdev(R011,R012,R013,R014,R015,R016,R017,R018,R019,R020)
s2 = 10.441

s3 := stdev(R12,R13,R14,R15,R16,R17,R18,R19,R23,R24)
s3 = 32.71

SS := mean(s1,s2,s3)
SS = 23.951
```

Рисунок 28 – Вычисление стандартного отклонения
расстояния Хемминга

Далее с помощью построения графиков в MathCad интерпретируем результаты численного эксперимента в график. Результат представлен на рисунке 29.

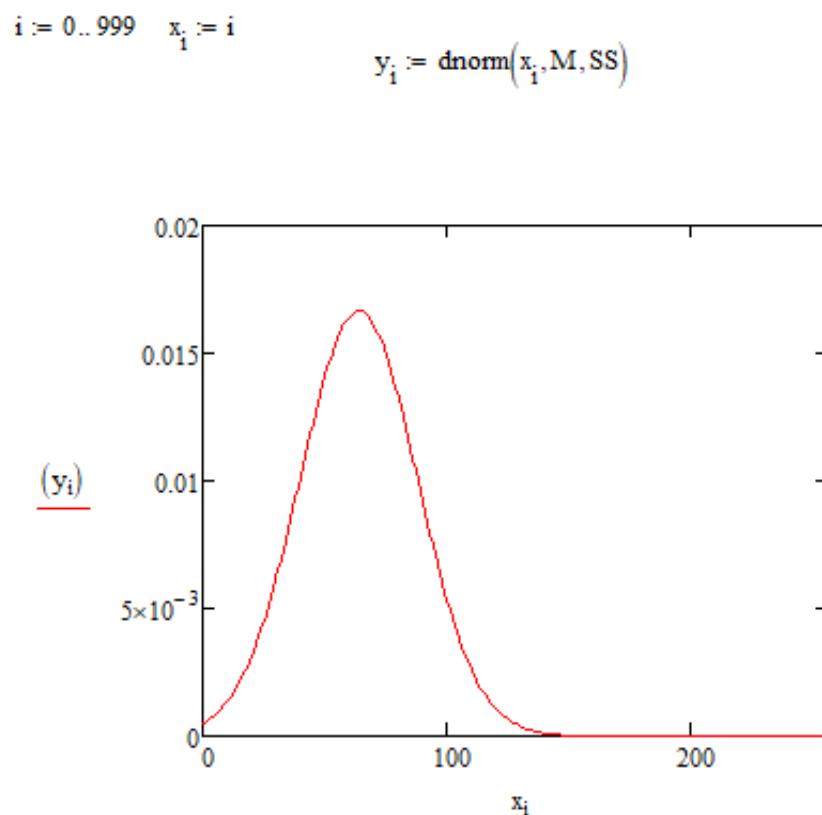


Рисунок 29 – Распределение расстояний Хемминга между ключами от примеров образов «Хонер»

Далее все эти операции повторяем с заранее подготовленными образами «Сура»:

- вычисление коэффициента корреляции между двумя векторами;
- вычисление математического ожидания;
- вычисление стандартного отклонения;
- интерпретация результатов численного эксперимента в график.

Результат приведен на рисунке 30 и в приложении В.

$i := 0..999 \quad x_i := i$
 $y_i := \text{dnorm}(x_i, M, SS)$

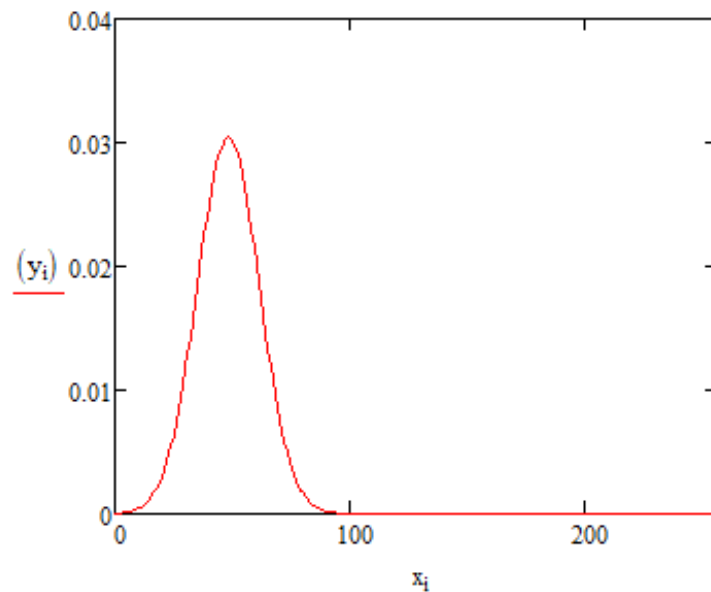


Рисунок 30 – Распределение расстояний Хемминга между ключами
от примеров образов «Сура»

Сравнивая полученные результаты численных экспериментов, мы видим, что корреляционная сцепленность 256 разрядов выходного кода нейросети для примеров биометрического образа «Чужой», выполненные двумя разными методиками, имеет одинаковый результат – образ «Свой» не достигнут.

5 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Профилактика и поддержание здоровья на протяжении всей жизни должны быть предметом первой необходимости и заботы людей разных возрастов и профессий.

В студенческом возрасте здоровье очень часто формируется под влиянием среды, в которой человек получает общение, и которое не всегда влияет положительно, однако в этот период происходит важный процесс становления ресурса развивающегося организма. Жизненные цели и ценности молодых людей сводятся к переосмыслению окружающего мира, ценностных представлений и мировоззрения в целом и формирования мотивации будущей профессиональной деятельности.

Организм человека – это развитая уникальная система состоящая из локальных систем, которые сформированы из органов, материальная часть которых включает клетки и внеклеточный матрикс (соединительную ткань). Локальные системы и их органы при совместном взаимодействии в рамках общей системы организма обеспечивают жизнь и здоровье человека.

Каждая локальная система выполняет свои функции, с помощью специальных медиаторов и других молекул клеточных коммуникаций, вырабатываемых клетками органов соответствующих подсистем.

Сердечно-сосудистая система человека – это комплекс органов, обеспечивающих снабжение всех участков организма (за небольшим исключением) необходимыми веществами и удаляющих продукты жизнедеятельности. Именно сердечно-сосудистая система обеспечивает все участки тела необходимым кислородом, а потому является основой жизни.

Сердечно-сосудистая система состоит из сердца, кровеносных сосудов (артерий, вен, кровеносных капилляров) и лимфатических сосудов. Сердце обеспечивает движение крови по кровеносным сосудам, состоит из четырех камер – правого предсердия и правого желудочка, левого предсердия и левого желудочка.

Заболевания сердечно-сосудистой системы являются актуальной медико-социальной проблемой, относящейся к приоритетам систем здравоохранения большинства стран мира.

Высокая частота встречаемости заболеваний сердечно-сосудистой системы в популяции, сопряженная с инвалидизацией и смертью больных, диктует необходимость своевременной диагностики и проведения адекватной терапии.

Увеличивающаяся распространенность болезни, связана с нервно-эмоциональным напряжением человека, с сидячим образом жизни, недостаточным количеством времени на свежем воздухе.

В сложившейся ситуации решение проблемы тесно сопряжено с четким определением задач, которые должны быть по возможности в максимальной степени реализованы при профилактике и лечении заболеваний сердечно-сосудистой системы.

Следует заметить, что профилактические мероприятия, связанные со здоровьем, и усилия, принимаемые при лечении болезней это разные понятия. Поэтому профилактические мероприятия, связанные с укреплением и поддержанием здоровья необходимо проводить вне зависимости от возникающих болезней, то есть в другой плоскости жизненных предпочтений.

Боль при заболеваниях сердечно-сосудистой системы носит приступообразный характер, появляясь, как правило, на фоне относительно благополучного состояния больного, что заставляет пациента сразу обратить на нее внимание, нередко вызывая выраженное беспокойство и страх.

Однако, достоверные исследования показали, что старая добрая физкультура и диета оказываются порой более эффективными в лечении и профилактике заболеваний сердечно-сосудистой системы, нежели медикаментозное лечение.

Основные физиологические условия нормальной работы организма:

– обеспечение катаболических процессов необходимыми питательными и другим веществами и их усвоения в целях получения низкомолекулярных соединений для последующих процессов обмена, а также веществ,

формирующих элементы клеточного матрикса.

- обеспечение окислительно восстановительных процессов пластического и энергетического обмена низкомолекулярными, промежуточными и другими соединениями в целях синтеза высокомолекулярных органических соединений (полимеров), энергетических молекул аденозинтрифосфат и медиаторов клеточных коммуникаций систем управления.

- обеспечение физиологических условий иммунной защиты клеточного матрикса от инфекций, токсинов и злокачественных перерождений;

- минимизация внешних и внутренних раздражителей, выступающих как нарушение гомеостаза и других проблем отдельно или в совокупности приводящих к патофизиологическим повреждениям в клеточном матриксе органов и систем управления.

- обеспечение оптимальных физиологических нагрузок (физических, когнитивных, психоэмоциональных) и режима релаксации (отдыха) в процессах жизнедеятельности человека;

Нарушения перечисленных условий могут привести к снижению жизненных ресурсов и эффективности функционирования органов и управляющих систем, а также энергетического потенциала организма в целом.

Исходя из данного определения стратегия физиологически грамотного отношения человека к своему организму, обеспечивающая качественные характеристики его здоровья будет заключаться в выполнении поставленных выше условий, которые необходимы для формирования, развития и сохранения физического и нравственного здоровья человека, в том числе специалистов по защите информации,

Заключение

Подводя итоги ВКР, можно сделать вывод, что решены все поставленные задачи и достигнута цель ВКР.

Проведен обзор нормативной документации по биометрической аутентификации в ходе которого установлено, что в России действует более 50 стандартов по нейросетевой статистической обработке биометрических данных: 44 международных стандарта комитета ISO/IEC JTC1 sc 37 (Биометрия) и семь национальных стандартов технического комитета 362 «Защита информации» Росстандарта России.

Проведен обзор методов биометрической аутентификации и средств тестирования биометрической аутентификации, в том числе среды моделирования «БиоНейроАвтограф».

В среде моделирования «БиоНейроАвтограф» были получены примеры образов «Чужой», представленные 21 рукописным словом «Хонер» и 21 рукописным образом «Сура». Выполнены обучение нейросети «БиоНейроАвтограф» и тестирование нейросети на ее стойкость к атаками подбора, пользуясь образами «Чужой» с формированием файлов ключей в виде строк бинарных состояний (256 бит) с определением ошибки второго рода P_2 .

С использованием среды математического моделирования MathCAD выполнены вычисления коэффициентов корреляции между длинными кодами, полученными примерами одного биометрического образа путем чтения достоверных данных, построены графики распределения коэффициентов корреляции для образов «Хонер» и «Сура».

В подтверждение результатов численного моделирования было создано программное обеспечение вычисляющее расстояния Хэмминга между анализируемыми кодовыми последовательностями по контрольной методике аспиранта Ратникова. В результате проделанной работы можно сделать вывод, что использование нейросетевых преобразователей биометрия-код повышает уровень защиты информации и стойкость к атакам подбора.

Для проведения дальнейших исследований в данной области рекомендовано модифицировать среду моделирования «БиоНейроАвтограф», которая является некоммерческим продуктом, разработанным лабораторией биометрических и нейросетевых технологий ОАО «ПНИЭИ» для высших учебных заведений России, путем добавления функции прямого вычисления коэффициентов корреляции.

По результатам дипломного проекта была написана статья: «Нейросетевая биометрия: подтверждение гипотезы обратных шкал для метрики корреляционной сцепленности и метрики расстояний Хэмминга при их применении к ключам-откликам на примере одного образа «Чужой» авторов К. А. Горбунова, В. В. Никитина, которая принята к публикации в сборнике научных статей по материалам III Всероссийской научно-технической конференции «Безопасность информационных технологий» и будет размещена в системе РИНЦ (Приложение Г).

На основании вышесказанного констатируем факт, что указ Президента России В. В. Путина № 490 от 10.10.2019 «О развитии искусственного интеллекта в Российской Федерации» выполняется.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены полностью.

Список используемых источников

1 Иванов А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции : монография. – Пенза : Изд-во АО «Пензенский научно- исследовательский электротехнический институт» (ОА «ПНИЭИ»), 2016. – 133 с.

2 Язов Ю.К., Волчихин В.И., Иванов А.И., Фунтиков В.А., Назаров И.Г. [и др.]. Нейросетевая защита персональных биометрических данных. – Москва : Радиотехника, 2012. – 157 с. – ISBN 978-5-88070-044-8.

3 Титов А. Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации [Электронный ресурс]. – URL: <https://securityrussia.com/blog/biometriya.html>

4 Биометрия в России: правовое регулирование и практика применения [Электронный ресурс]. – URL: https://www.antimalware.ru/analytics/Technology_Analysis/Biometrics-in-Russia.

5 Иванов А. И. Среда моделирования «БиоНейроАвтограф» : учеб.-метод. пособие – Пенза : Изд-во ПГУ, 2020. – 60 с.

6 ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к высоконадежным средствам биометрической аутентификации. – Москва, 2006.

7 ГОСТ Р 52633.1–2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. – Москва, 2009.

8 ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. – Москва, 2010.

9 ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. – Москва, 2011.

10 ГОСТ Р 52633.4–2011. Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа. – Москва, 2011.

11 ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. – Москва, 2011.

12 ГОСТ Р 52633.6–2012. Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой». – Москва, 2012.

13 Волчихин В.И., Малыгин А.Ю., Лупанов М.Ю., Семенов А.В. О проблеме ресурсов при тестировании стойкости высоконадежных биометрических технологий // Вопросы защиты информации. – 2006. – № 4. – С. 15–16.

14 Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования высоконадежных нейросетевых механизмов биометрико-криптографической защиты информации : монография. – Пенза : Изд-во Пенз. гос. ун-та, 2006. – 160 с.

15 ГОСТ Р 50779.21–2004. Статистические методы. Правила определения и методы расчета статистических характеристик по выборочным данным. Часть 1. Нормальное распределение. – Москва, 2004.

16 Иванов А. И., Иванов А. П., Ратников К. А. Статистико-нейросетевой анализ биометрических образов в пространствах спектров кроссверток и автосверток Хэмминга : препринт. – Пенза : Изд-во ПГУ, 2021. – 56 с.

17 Ахметов Б.С., Иванов А.И., Фунтиков В.А., Малыгин А.Ю. Основы биометрической идентификации личности : учебное пособие. – Алматы : КазНТУ им. К.И. Сатпаева, 2014. – 151 с. – ISBN 978-601-228-689-2

18 Волчихин В.И., Ахметов Б.Б., Иванов А.И. Быстрый алгоритм симметризации корреляционных связей биометрических данных высокой размерности // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2016. – № 1. – С. 3–7.

Приложение А (обязательное)

Международные биометрические стандарты, действующие на территории РФ

Таблица А.1 – ИСО/МЭК СТК 1/ПК 37 (ISO/IEC JTC1 SC37)

29109 - Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794	
ISO/IEC 29109-1:2009 Information technology — Biometrics — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology	ГОСТ Р ИСО/МЭК 29109-1-2012 Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 1. Обобщенная методология испытаний на соответствие
ISO/IEC 29109-4:2010 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 4: Finger image data	ГОСТ Р ИСО/МЭК 29109-4-2015 Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 4. Данные изображения отпечатка пальца
ISO/IEC 29109-5:2014 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 5: Face image data	ГОСТ Р ИСО/МЭК 29109-5-2013 Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 5. Данные изображения лица
ISO/IEC 29109-6:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 6: Iris image data	ГОСТ Р ИСО/МЭК 29109-6-2016 Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 6. Данные изображения радужной оболочки глаза
ISO/IEC 29109-7:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 7: Signature/sign time series data	ГОСТ Р ИСО/МЭК 29109-7-2016 Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 7. Данные динамики подписи
ISO/IEC 29109-8:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 8: Finger pattern skeletal data	ГОСТ Р ИСО/МЭК 29109-8-2016 Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 8. Данные изображения отпечатка пальца — остов
19785 - Единая структура форматов обмена биометрическими данными	
ISO/IEC 19785-1:2015 Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification	ГОСТ Р ИСО/МЭК 19785-1-2008 Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных
ISO/IEC 19785-2:2006 Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority	ГОСТ Р ИСО/МЭК 19785-2-2008 Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии
ISO/IEC 19785-4:2010 Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications	ГОСТ Р ИСО/МЭК 19785-4-2012 Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 4. Спецификация формата блока защиты информации
19784 - Биометрический программный интерфейс (BioAPI)	
ISO/IEC 19784-1:2006 Information technology — Biometric application programming interface — Part 1: BioAPI specification	ГОСТ Р ИСО/МЭК 19784-1-2007 Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса

Продолжение таблицы А1

Обозначение и название стандарта на английском языке	Обозначение и название стандарта на русском языке
19794 - Форматы обмена биометрическими данными	
ISO/IEC 19794-1:2006 Information technology — Biometric data interchange formats — Part 1: Framework	ГОСТ ISO/IEC 19794-1-2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура
ISO/IEC 19794-2:2005 Information technology — Biometric data interchange formats — Part 2: Finger minutiae data	ГОСТ Р ИСО/МЭК 19794-2-2013 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки
ISO/IEC 19794-3:2006 Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data	ГОСТ Р ИСО/МЭК 19794-3-2009 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца
ISO/IEC 19794-4:2005 Information technology — Biometric data interchange formats — Part 4: Finger image data	ГОСТ Р ИСО/МЭК 19794-4-2014 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца
ISO/IEC 19794-5:2005 Information technology — Biometric data interchange formats — Part 5: Face image data	ГОСТ Р ИСО/МЭК 19794-5-2013 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица
ISO/IEC 19794-6:2005 Information technology — Biometric data interchange formats — Part 6: Iris image data	ГОСТ Р ИСО/МЭК 19794-6-2014 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза
ISO/IEC 19794-7:2007 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data	ГОСТ Р ИСО/МЭК 19794-7-2009 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи
ISO/IEC 19794-8:2006 Information technology — Biometric data interchange formats — Part 8: Finger pattern skeletal data	ГОСТ Р ИСО/МЭК 19794-8-2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 8. Данные изображения отпечатка пальца — остов
ISO/IEC 19794-9:2007 Information technology — Biometric data interchange formats — Part 9: Vascular image data	ГОСТ Р ИСО/МЭК 19794-9-2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла
ISO/IEC 19794-10:2007 Information technology — Biometric data interchange formats — Part 10: Hand geometry silhouette data	ГОСТ Р ИСО/МЭК 19794-10-2010 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки
ISO/IEC 19794-11:2013 Information technology — Biometric data interchange formats — Part 11: Signature/sign processed dynamic data	ГОСТ Р ИСО/МЭК 19794-11-2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Обработываемые данные динамики подписи
ISO/IEC 19794-14 Information technology — Biometric data interchange formats — Part 14: DNA data, IDT	ГОСТ Р ИСО/МЭК 19794-14 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК

Продолжение таблицы А1

ISO/IEC 19784-2:2007 Information technology — Biometric application programming interface — Part 2: Biometric archive function provider interface	ГОСТ Р ИСО/МЭК 19784-2-2010 Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 2. Интерфейс поставщика биометрической функции архива
ISO/IEC 19784-4:2011 Information technology — Biometric application programming interface — Part 4: Biometric sensor function provider interface	ГОСТ Р ИСО/МЭК 19784-4-2014 Информационные технологии. Биометрия. Биометрический программный интерфейс. Часть 4. Интерфейс поставщика функции биометрического датчика
24708, 24709 - Протокол межсетевого обмена БиоАПИ	
ISO/IEC 24708:2008 Information technology — Biometrics — BioAPI Interworking Protocol	ГОСТ Р ИСО/МЭК 24708-2013 Информационные технологии. Биометрия. Протокол межсетевого обмена БиоАПИ
ISO/IEC 24709-1:2007 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures	ГОСТ Р ИСО/МЭК 24709-1-2009 Автоматическая идентификация. Идентификация биометрическая. Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ). Часть 1. Методы и процедуры
ISO/IEC 24709-2:2007 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 2: Test assertions for biometric service providers	ГОСТ Р ИСО/МЭК 24709-2-2011 Информационные технологии. Биометрия. Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ). Часть 2. Тестовые утверждения для поставщиков биометрических услуг
ISO/IEC 24709-3:2011 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 3: Test assertions for BioAPI frameworks	ГОСТ Р ИСО/МЭК 24709-3-2013 Информационные технологии. Биометрия. Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ). Часть 3. Тестовые утверждения для инфраструктур БиоАПИ
24713 - Биометрические профили для взаимодействия и обмена данными	
ISO/IEC 24713-1:2008 Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles	ГОСТ ISO/IEC 24713-1-2013 Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили
ISO/IEC 24713-2:2008 Information technology — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports	ГОСТ Р ИСО/МЭК 24713-2-2011 Информационные технологии. Биометрия. Биометрические профили для взаимодействия и обмена данными. Часть 2. Физический контроль доступа сотрудников аэропорта
ISO/IEC 24713-3:2009 Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometrics-based verification and identification of seafarers	ГОСТ Р ИСО/МЭК 24713-3-2016 Информационные технологии. Биометрия. Биометрические профили для взаимодействия и обмена данными. Часть 3. Биометрическая верификация и идентификация моряков
19795 - Эксплуатационные испытания и протоколы испытаний в биометрии	
ISO/IEC 19795-1:2006 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework	ГОСТ Р ИСО/МЭК 19795-1-2007 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура
ISO/IEC 19795-2:2007 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation	ГОСТ Р ИСО/МЭК 19795-2-2008 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний
ISO/IEC TR 19795-3:2007 Information technology — Biometric performance testing and reporting — Part 3: Modality-specific testing	ГОСТ Р ИСО/МЭК ТО 19795-3-2009 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3. Особенности проведения испытаний при различных биометрических модальностях

Продолжение таблицы А1

ISO/IEC 19795-4:2008 Information technology — Biometric performance testing and reporting — Part 4: Interoperability performance testing	ГОСТ Р ИСО/МЭК 19795-4-2011 Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Испытания на совместимость
ISO/IEC 19795-6:2012 Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation	ГОСТ Р ИСО/МЭК 19795-6-2015 Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 6. Методология проведения оперативных испытаний
Другие различные стандарты	
ISO/IEC 2382-37:2012 Information technology — Vocabulary — Part 37: Biometrics	ГОСТ ISO/IEC 2382-37-2016 Информационные технологии. Словарь. Часть 37. Биометрия
ISO/IEC 29794-1:2016 Information technology — Biometric sample quality — Part 1: Framework	ГОСТ Р ИСО/МЭК 29794-1-2012 Информационные технологии. Биометрия. Качество биометрических образцов. Часть 1. Структура
ISO/IEC 29141:2009 Information technology — Biometrics — Tenprint capture using biometric application programming interface (BioAPI)	ГОСТ Р ИСО/МЭК 29141-2012 Информационные технологии. Биометрия. Одновременное получение изображений отпечатков десяти пальцев с помощью БиоАПИ
ISO/IEC TR 24741:2007 Information technology — Biometrics tutorial	ГОСТ Р 54412-2011/ISO/IEC TR 24741:2007 Информационные технологии. Биометрия. Обучающая программа по биометрии
ISO/IEC TR 24722:2015 Information technology — Biometrics — Multimodal and other multibiometric fusion	ГОСТ Р 54411-2011/ISO/IEC TR 24722:2007 Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии
ISO/IEC 7816-11:2004 Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods	ГОСТ Р ИСО/МЭК 7816-11-2013 Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами
ISO/IEC 11694-6:2014 Identification cards — Optical memory cards — Linear recording method — Part 6: Use of biometrics on an optical memory card	ГОСТ Р ИСО/МЭК 11694-6-2011 Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 6. Использование биометрических данных на картах с оптической памятью
ISO/IEC 29159-1:2010 Information technology — Biometric calibration, augmentation and fusion data — Part 1: Fusion information format, IDT	ГОСТ Р ИСО/МЭК 29159-1— 2017 Информационные технологии. Биометрия. Калибровка, аугментация и объединение данных в биометрии. Часть 1. Формат объединения данных

Приложение Б (обязательное)

Алгоритм численного эксперимента оценки корреляционной сцепленности между ключами от примеров образа «Сура»

```

x0 := READPRN("Cypa1.txt")      last(x0) = 255
x1 := READPRN("Cypa2.txt")      x12 := READPRN("Cypa13.txt")
x2 := READPRN("Cypa3.txt")      x13 := READPRN("Cypa14.txt")
x3 := READPRN("Cypa4.txt")      x14 := READPRN("Cypa15.txt")
x4 := READPRN("Cypa5.txt")      x15 := READPRN("Cypa16.txt")
x5 := READPRN("Cypa6.txt")      x16 := READPRN("Cypa17.txt")
x6 := READPRN("Cypa7.txt")      x17 := READPRN("Cypa18.txt")
x7 := READPRN("Cypa8.txt")      x18 := READPRN("Cypa19.txt")
x8 := READPRN("Cypa9.txt")      x19 := READPRN("Cypa20.txt")
x9 := READPRN("Cypa10.txt")     x20 := READPRN("Cypa21.txt")
x10 := READPRN("Cypa11.txt")    x21 := READPRN("Cypa1.txt")
x11 := READPRN("Cypa12.txt")

x0T =


|   |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |     |
|---|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|-----|
|   | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18  |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0  | 0  | 0  | 1  | 1  | 0  | 1  | 0  | ... |



Вычисление коэффициентов корреляции между двумя векторами

R01 := corr(x0,x1)      corr(x0,x1) = 0.439
R02 := corr(x0,x2)
R03 := corr(x0,x3)
R04 := corr(x0,x4)
R05 := corr(x0,x5)
R06 := corr(x0,x6)
R07 := corr(x0,x7)
R08 := corr(x0,x8)
R09 := corr(x0,x9)
R10 := corr(x0,x10)
R11 := corr(x0,x11)
R12 := corr(x0,x12)
R13 := corr(x0,x13)
R14 := corr(x0,x14)
R15 := corr(x0,x15)
R16 := corr(x0,x16)
R17 := corr(x0,x17)
R18 := corr(x0,x18)
R19 := corr(x0,x19)
R20 := corr(x0,x20)
R21 := corr(x0,x21)
R12 := corr(x1,x2)
R13 := corr(x1,x3)
R14 := corr(x1,x4)
R15 := corr(x1,x5)
R16 := corr(x1,x6)
R17 := corr(x1,x7)
R18 := corr(x1,x8)
R19 := corr(x1,x9)
R20 := corr(x1,x10)
R21 := corr(x1,x11)
R22 := corr(x1,x12)
R23 := corr(x1,x13)
R24 := corr(x1,x14)
R25 := corr(x1,x15)
R26 := corr(x1,x16)
R27 := corr(x1,x17)
R28 := corr(x1,x18)
R29 := corr(x1,x19)
R30 := corr(x1,x20)
R31 := corr(x1,x21)
R32 := corr(x2,x3)
R33 := corr(x2,x4)
R34 := corr(x2,x5)
R35 := corr(x2,x6)
R36 := corr(x2,x7)
R37 := corr(x2,x8)
R38 := corr(x2,x9)
R39 := corr(x2,x10)
R40 := corr(x2,x11)
R41 := corr(x2,x12)
R42 := corr(x2,x13)
R43 := corr(x2,x14)
R44 := corr(x2,x15)
R45 := corr(x2,x16)
R46 := corr(x2,x17)
R47 := corr(x2,x18)
R48 := corr(x2,x19)
R49 := corr(x2,x20)
R50 := corr(x2,x21)
R51 := corr(x3,x4)
R52 := corr(x3,x5)
R53 := corr(x3,x6)
R54 := corr(x3,x7)
R55 := corr(x3,x8)
R56 := corr(x3,x9)
R57 := corr(x3,x10)
R58 := corr(x3,x11)
R59 := corr(x3,x12)
R60 := corr(x3,x13)
R61 := corr(x3,x14)
R62 := corr(x3,x15)
R63 := corr(x3,x16)
R64 := corr(x3,x17)
R65 := corr(x3,x18)
R66 := corr(x3,x19)
R67 := corr(x3,x20)
R68 := corr(x3,x21)
R69 := corr(x4,x5)
R70 := corr(x4,x6)
R71 := corr(x4,x7)
R72 := corr(x4,x8)
R73 := corr(x4,x9)
R74 := corr(x4,x10)
R75 := corr(x4,x11)
R76 := corr(x4,x12)
R77 := corr(x4,x13)
R78 := corr(x4,x14)
R79 := corr(x4,x15)
R80 := corr(x4,x16)
R81 := corr(x4,x17)
R82 := corr(x4,x18)
R83 := corr(x4,x19)
R84 := corr(x4,x20)
R85 := corr(x4,x21)
R86 := corr(x5,x6)
R87 := corr(x5,x7)
R88 := corr(x5,x8)
R89 := corr(x5,x9)
R90 := corr(x5,x10)
R91 := corr(x5,x11)
R92 := corr(x5,x12)
R93 := corr(x5,x13)
R94 := corr(x5,x14)
R95 := corr(x5,x15)
R96 := corr(x5,x16)
R97 := corr(x5,x17)
R98 := corr(x5,x18)
R99 := corr(x5,x19)
R100 := corr(x5,x20)
R101 := corr(x5,x21)
R102 := corr(x6,x7)
R103 := corr(x6,x8)
R104 := corr(x6,x9)
R105 := corr(x6,x10)
R106 := corr(x6,x11)
R107 := corr(x6,x12)
R108 := corr(x6,x13)
R109 := corr(x6,x14)
R110 := corr(x6,x15)
R111 := corr(x6,x16)
R112 := corr(x6,x17)
R113 := corr(x6,x18)
R114 := corr(x6,x19)
R115 := corr(x6,x20)
R116 := corr(x6,x21)
R117 := corr(x7,x8)
R118 := corr(x7,x9)
R119 := corr(x7,x10)
R120 := corr(x7,x11)
R121 := corr(x7,x12)
R122 := corr(x7,x13)
R123 := corr(x7,x14)
R124 := corr(x7,x15)
R125 := corr(x7,x16)
R126 := corr(x7,x17)
R127 := corr(x7,x18)
R128 := corr(x7,x19)
R129 := corr(x7,x20)
R130 := corr(x7,x21)
R131 := corr(x8,x9)
R132 := corr(x8,x10)
R133 := corr(x8,x11)
R134 := corr(x8,x12)
R135 := corr(x8,x13)
R136 := corr(x8,x14)
R137 := corr(x8,x15)
R138 := corr(x8,x16)
R139 := corr(x8,x17)
R140 := corr(x8,x18)
R141 := corr(x8,x19)
R142 := corr(x8,x20)
R143 := corr(x8,x21)
R144 := corr(x9,x10)
R145 := corr(x9,x11)
R146 := corr(x9,x12)
R147 := corr(x9,x13)
R148 := corr(x9,x14)
R149 := corr(x9,x15)
R150 := corr(x9,x16)
R151 := corr(x9,x17)
R152 := corr(x9,x18)
R153 := corr(x9,x19)
R154 := corr(x9,x20)
R155 := corr(x9,x21)
R156 := corr(x10,x11)
R157 := corr(x10,x12)
R158 := corr(x10,x13)
R159 := corr(x10,x14)
R160 := corr(x10,x15)
R161 := corr(x10,x16)
R162 := corr(x10,x17)
R163 := corr(x10,x18)
R164 := corr(x10,x19)
R165 := corr(x10,x20)
R166 := corr(x10,x21)
R167 := corr(x11,x12)
R168 := corr(x11,x13)
R169 := corr(x11,x14)
R170 := corr(x11,x15)
R171 := corr(x11,x16)
R172 := corr(x11,x17)
R173 := corr(x11,x18)
R174 := corr(x11,x19)
R175 := corr(x11,x20)
R176 := corr(x11,x21)
R177 := corr(x12,x13)
R178 := corr(x12,x14)
R179 := corr(x12,x15)
R180 := corr(x12,x16)
R181 := corr(x12,x17)
R182 := corr(x12,x18)
R183 := corr(x12,x19)
R184 := corr(x12,x20)
R185 := corr(x12,x21)
R186 := corr(x13,x14)
R187 := corr(x13,x15)
R188 := corr(x13,x16)
R189 := corr(x13,x17)
R190 := corr(x13,x18)
R191 := corr(x13,x19)
R192 := corr(x13,x20)
R193 := corr(x13,x21)
R194 := corr(x14,x15)
R195 := corr(x14,x16)
R196 := corr(x14,x17)
R197 := corr(x14,x18)
R198 := corr(x14,x19)
R199 := corr(x14,x20)
R200 := corr(x14,x21)
R201 := corr(x15,x16)
R202 := corr(x15,x17)
R203 := corr(x15,x18)
R204 := corr(x15,x19)
R205 := corr(x15,x20)
R206 := corr(x15,x21)
R207 := corr(x16,x17)
R208 := corr(x16,x18)
R209 := corr(x16,x19)
R210 := corr(x16,x20)
R211 := corr(x16,x21)
R212 := corr(x17,x18)
R213 := corr(x17,x19)
R214 := corr(x17,x20)
R215 := corr(x17,x21)
R216 := corr(x18,x19)
R217 := corr(x18,x20)
R218 := corr(x18,x21)
R219 := corr(x19,x20)
R220 := corr(x19,x21)
R221 := corr(x20,x21)

Вычисление Мат. Ожиданий

m1 := mean(R01,R02,R03,R04,R05,R06,R07,R08,R09,R10)
m1 = 0.532

m2 := mean(R011,R012,R013,R014,R015,R016,R017,R018,R019,R20)
m2 = 0.557

m3 := mean(R12,R13,R14,R15,R16,R17,R18,R19,R23,R24)
m3 = 0.666

M := mean(m1,m2,m3)
M = 0.585

Вычисление стандартного отклонения

s1 := stdev(R01,R02,R03,R04,R05,R06,R07,R08,R09,R10)
s1 = 0.054

s2 := stdev(R011,R012,R013,R014,R015,R016,R017,R018,R019,R20)
s2 = 0.073

s3 := stdev(R12,R13,R14,R15,R16,R17,R18,R19,R23,R24)
s3 = 0.1

SS := mean(s1,s2,s3)
SS = 0.075

i := 0..999  xi := 0.01 · i
yi := dnorm(xi,M,SS)

```

Приложение В (обязательное)

Алгоритм численного эксперимента оценки корреляционной сцепленности между ключами от примеров образа «Сура» в пространстве расстояний Хемминга

Вычисление_коэффициентов_корреляции_между_двумя_векторами

$$\begin{aligned}
 R01 &:= \sum_{i=0}^{255} (x0_i \oplus x1_i) & R02 &:= \sum_{i=0}^{255} (x0_i \oplus x2_i) & R03 &:= \sum_{i=0}^{255} (x0_i \oplus x3_i) \\
 R04 &:= \sum_{i=0}^{255} (x0_i \oplus x4_i) & R05 &:= \sum_{i=0}^{255} (x0_i \oplus x5_i) & R06 &:= \sum_{i=0}^{255} (x0_i \oplus x6_i) \\
 R07 &:= \sum_{i=0}^{255} (x0_i \oplus x7_i) & R08 &:= \sum_{i=0}^{255} (x0_i \oplus x8_i) & R09 &:= \sum_{i=0}^{255} (x0_i \oplus x9_i) \\
 R10 &:= \sum_{i=0}^{255} (x0_i \oplus x10_i) & R11 &:= \sum_{i=0}^{255} (x0_i \oplus x11_i) & R12 &:= \sum_{i=0}^{255} (x0_i \oplus x12_i) \\
 R13 &:= \sum_{i=0}^{255} (x0_i \oplus x13_i) & R14 &:= \sum_{i=0}^{255} (x0_i \oplus x14_i) & R15 &:= \sum_{i=0}^{255} (x0_i \oplus x15_i) \\
 R16 &:= \sum_{i=0}^{255} (x0_i \oplus x16_i) & R17 &:= \sum_{i=0}^{255} (x0_i \oplus x17_i) & R18 &:= \sum_{i=0}^{255} (x0_i \oplus x18_i) \\
 & & & & R19 &:= \sum_{i=0}^{255} (x0_i \oplus x19_i) \\
 & & & & R20 &:= \sum_{i=0}^{255} (x0_i \oplus x20_i) \\
 & & & & R21 &:= \sum_{i=0}^{255} (x1_i \oplus x2_i) \\
 R13 &:= \sum_{i=0}^{255} (x1_i \oplus x3_i) & R14 &:= \sum_{i=0}^{255} (x1_i \oplus x4_i) & R15 &:= \sum_{i=0}^{255} (x1_i \oplus x5_i) \\
 R16 &:= \sum_{i=0}^{255} (x1_i \oplus x6_i) & R17 &:= \sum_{i=0}^{255} (x1_i \oplus x7_i) & & \\
 & & & & R23 &:= \sum_{i=0}^{255} (x1_i \oplus x18_i) \\
 & & & & R24 &:= \sum_{i=0}^{255} (x1_i \oplus x19_i)
 \end{aligned}$$

Вычисление Мат. Ожиданий.

$$\begin{aligned}
 m1 &:= \text{mean}(R01, R02, R03, R04, R05, R06, R07, R08, R09, R10) & m1 &= 59.8 \\
 m2 &:= \text{mean}(R11, R12, R13, R14, R15, R16, R17, R18, R19, R20) & m2 &= 56.6 \\
 m3 &:= \text{mean}(R21, R23, R24) & m3 &= 28.083 \\
 M &:= \text{mean}(m1, m2, m3) & M &= 48.161
 \end{aligned}$$

Вычисление стандартного отклонения

$$\begin{aligned}
 s1 &:= \text{stdev}(R01, R02, R03, R04, R05, R06, R07, R08, R09, R10) & s1 &= 7.011 \\
 s2 &:= \text{stdev}(R11, R12, R13, R14, R15, R16, R17, R18, R19, R20) & s2 &= 9.372 \\
 s3 &:= \text{stdev}(R21, R23, R24) & s3 &= 22.947 \\
 SS &:= \text{mean}(s1, s2, s3) & SS &= 13.11
 \end{aligned}$$

Приложение Г
(справочное)

Статья, принятая к публикации в сборнике научных статей
по материалам III Всероссийской научно-технической конференции
«Безопасность информационных технологий» (г. Пенза, 4 июня 2021 г.)

Горбунов К. А., Никитин В. В.

**НЕЙРОСЕТЕВАЯ БИОМЕТРИЯ: ПОДТВЕРЖДЕНИЕ ГИПОТЕЗЫ ОБРАТНЫХ ШКАЛ
ДЛЯ МЕТРИКИ КОРРЕЛЯЦИОННОЙ СЦЕПЛЕННОСТИ И МЕТРИКИ РАССТОЯНИЙ
ХЭММИНГА ПРИ ИХ ПРИМЕНЕНИИ К КЛЮЧАМ-ОТКЛИКАМ НА ПРИМЕРЫ
ОДНОГО ОБРАЗА «ЧУЖОЙ»**

При тестировании стойкости к атакам подбора рукописных образов среды моделирования «БиоНейроАвтограф» [1, 2] могут быть выбраны разные образы «Чужой». Например, если мы выбираем при тестировании 21 пример рукописного образа «Хопер», то получаем математическое ожидание коэффициентов корреляционной сцепленности $E(r) \approx 0.43$, что отображено в левой части рисунка 1. Если же мы будем выполнять тестирование на примерах рукописного образа «Сура», то порождаемые этим образом ключи (длина ключа 256 бит) дают более высокий уровень корреляционной сцепленности $E(r) \approx 0.59$. Это означает, что примеры образа «Сура» ближе к образу «Свой», так как образ «Свой» обладает предельно высокой корреляционной сцепленностью с единичным математическим ожиданием $E(r) \approx 1.0$. Эта ситуация отображена на рисунке 1.

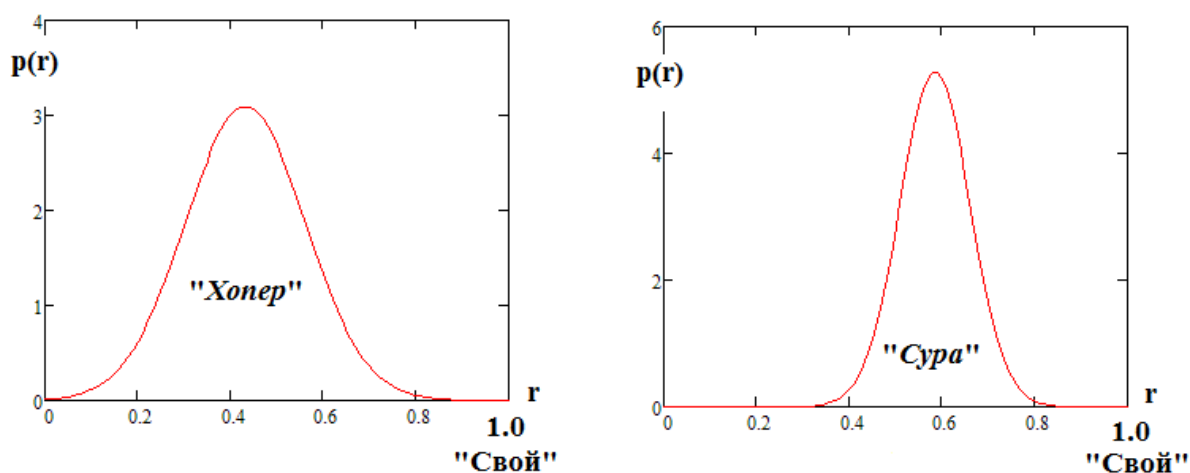


Рис. 1. Распределение расстояний корреляционной сцепленности между ключами от примеров образа Хопер (предельное значение корреляции «Свой» в правой части рисунка $r=1.0$)

При вычислениях данных рисунка 1 корреляционная метрика вычислялась как функция $\text{corr}(x_j, x_i)$, где i, j – номера примеров, порождающих коды отклики тестируемых образов.

Совершенно иная ситуация возникает, если мы будем рассматривать кодовые ключи отклики на тестовые образы в пространстве расстояний Хэмминга (в пространстве автосверток Хэмминга [3]). Эта ситуация отображена на рисунке 2.

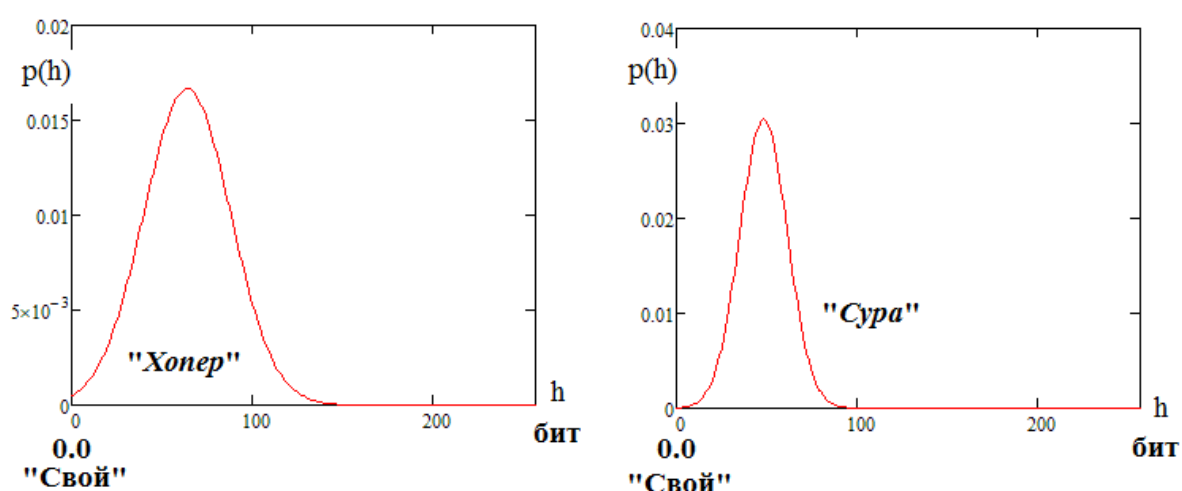


Рис. 2. Распределение расстояний Хемминга между ключами от примеров образа Хонер (предельное значение «Свой» в левой части рисунка $h=0.0$)

Из рисунка 2 видно, что две рассматриваемые метрики обратны. Математическое ожидание Хэмминговых автосверток составляет $E(h) \approx 86$ бит для примеров образа «Хонер». Для 21 примера образа «Сура» математическое ожидание сверток Хэмминга существенно меньше $E(h) \approx 86$ бит. В целом метрика корреляционной сцепленности (рис. 1) и метрика автосверток Хэмминга ведут себя похоже, однако образ «Свой» $E(r) \approx 1.0$ и $E(h) \approx 0.0$ находятся с разных сторон по отношению к математическим ожиданиям двух разных метрик. Фактически рассматриваемые метрики обладают обратными шкалами, то есть являются слабо независимыми.

Список литературы

1. Иванов А.И., Захаров О.С. Среда моделирования «БиоНейроАвтограф». Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ». URL: <http://пниэи.рф/activity/science/noc/bioneuroautograph.zip> [Для свободного использования университетами России, Белоруссии, Казахстана].
2. Иванов А.И. Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях : учеб. пособие. Пенза, 2013. 30 с. URL: http://пниэи.рф/activity/science/noc/tm_IvanovAI.pdf
3. Иванов А.И., Иванов А.П., Ратников К.А. Статистико-нейросетевой анализ биометрических образов в пространствах сверток и автосверток Хэмминга : препринт. Пенза : Изд-во ПГУ, 2021. 56 с. ISBN 978-5-907364-94-3



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный университет»
(ФГБОУ ВО «ПГУ»)

Красная ул., д. 40, г. Пенза, Россия, 440026.
Тел/факс: (841-2) 66-63-32, e-mail: cnit@pnzgu.ru, <http://www.pnzgu.ru>
ОКПО 02069042, ОГРН 1025801440620, ИНН/КПП 5837003736/583701001

28.06.2012 № 14-656
На № _____ от _____

Настоящим удостоверяем, что статья «Нейросетевая биометрия: подтверждение гипотезы обратных шкал для метрики корреляционной сцепленности и метрики расстояний Хэмминга при их применении к ключам-откликам на примере одного образа «Чужой» авторов К. А. Горбунова, В. В. Никитина, включена в сборник научных статей по материалам III Всероссийской научно-технической конференции «Безопасность информационных технологий» и будет размещена в системе РИНЦ.

Проректор по учебной работе



В. Б. Механов