УДК 004.056.5

В.Ж.Тулемисова[1,a], А.С.Бижанова[1,b]
[1]Казахская академия транспорта и коммуникаций имени М.Тынышпаева, г.Алматы, Казахстан
[a]almasaltyn@mail.ru, [b]vtulemisova@mail.ru

АЛГОРИТМЫ ОЦЕНКИ ИНФОРМАТИВНОСТИ БИОМЕТРИЧЕСКИХ ОБРАЗОВ И ИХ СТОЙКОСТИ ЗАЩИТЫ

Аннотация. Стремительная информатизация современного общества приводит к появлению новых проблем и новых подходов к их решению. В любой открытой достоверной информации размыта конфиденциальная информация. Порою лица, ведущие открытую (не защищенную) деловую переписку, даже не подозревают о том, что формируют пласты богатой информации, достаточно удобной для последующего извлечения из нее конфиденциальных данных.

Аңдатпа. Қарқынды ақпараттандыру қазіргі қоғамда жаңа проблемалар мен оларды шешудің жаңа тәсілдерінің пайда болуына әкеледі. Кез келген ашық және сенімді ақпараттардан құпия ақпарат алынады. Кейде адамдар, ашық (қорғалмаған) іскерлік хат алмасудан оның ішіндегі ақпараттардан құпияға бай деректерді алуға болатындығын байқамайды да.

Abstract. The rapid computerization of modern society leads to the emergence of new problems and new approaches to their solution. In any open reliable information blurred confidential information. The person leading the open (not secure) business correspondence, do not even know thow forming the seams of rich information, which the enough for later retrieval from it confidential data.

Ключевые слова: информационная безопасность, защита информации, биометрические технологии, биометрический образ, клавиатурный почерк, рукописный почерк, стойкость защиты, стабильность.

Түйінді сөздер: ақпараттық қауіпсіздік, ақпаратты қорғау, биометриялық технологиялар, биометрикалық бейнесі, пернетақтамен жазу, қолжазба жазу мәнері, тұрақтылық.

Keywords: biometric images, handwriting keyboard, handwriting, annotation.

Одним из путей защиты информационного пространства России и Казахстана является массовое использование криптографической защиты, например, при ведении деловой электронной переписки между государственными предприятиями и переписки между сотрудниками госпредприятий. При этом система защиты не должна мешать пользователям, затрудняя их работу. Система должна быть дружественной к пользователям, криптографические механизмы защиты должны быть невидимыми для них. Стойкость защиты может быть не очень высокой, но она должна быть тотальной для легитимных пользователей. Однако данный подход является эффективным именно для корпоративного применения, когда действия сотрудников могут быть четко регламентированы внутренними инструкциями с установленными мерами ответственности. При массовом использовании криптографии возникают проблемы как распределения и хранения личных ключей миллионов пользователей, так и человеческий фактор, обусловленный как привычкой, так и забывчивостью в том числе и отношении хранения ключей. Эту задачу не удается решить традиционными методами [1,2].

Основной задачей биометрии является создание устройств и программ, способных с высокой вероятностью идентифицировать пользователя системы по и с еще более высокой вероятностью распознавать злоумышленников, пытающихся маскироваться под легальных пользователей.

Большинство современных систем разграничения доступа основаны на привязки к различным статичными характеристикам пользователя.

К таким статическим образам относятся: геометрия лица (анфас, профиль, объемная геометрия); геометрия ушных раковин; тепловой портрет лица; геометрия руки; рисунок кровеносных сосудов глазного дна; рисунок вен на запястье руки; рисунок радужных оболочек глаз (разные рисунки у каждого глаза); рисунок кожных покровов подушечек пальцев и ладоней; генотип и следы пота [1,3].

Все перечисленные выше биометрические образы личности – открыты и следовательно легко имитируемы. Контактируя с конкретным человеком, легко получить образцы его отпечатков пальцев, геометрии руки, лица и т.д. В силу этого протоколы биометрической аутентификации, построенные на использовании открытых (доступных для наблюдения всеми) биометрических образов, должны быть защищены от предъявления муляжей. Как правило, такая защита может быть эффективной далеко не всегда. Кроме того, биометрические устройства и программы, использующие открытые биометрические образы человека, должны быть физически защищены. Надежность таких устройств целиком опирается на достижимую в данный момент чувствительность выбранного биометрического метода и стабильность измеряемых параметров [3-5].

Как правило, вероятность ошибки первого рода (ложный отказ в аутентификации «своему») для биометрии открытых образов составляет от 0,01 до 0,04. Вероятность ошибки второго рода (ошибочной аутентификации «чужого») составляет от 10^{-2} до 10^{-6}. При этом если уровень 0,01 для ошибок первого рода можно считать приемлемым, а уровень ошибок второго рода -10^{-6} недостаточно мал для многих важных приложений. Тенденция по объединению в одном устройстве нескольких статических биометрических технологий активно поддерживается многими фирмами, но этот подход дорог и не спасает положения.

Наиболее перспективным решением задачи повышения надежности является отказ от использования при аутентификации открытых биометрических образов. Таким образом злоумышленник лишается возможности предъявления биометрическим системам синтезированного им муляжа заранее известного биометрического образа. Основой безопасности протоколов становится сохранение в тайне биометрического образа, технические характеристики биометрических систем начинают играть второстепенную роль. За счет сохранения тайны биометрии и природной сложности тайных биометрических образов может быть обеспечен любой заданный уровень информационной безопасности.

Основными направлениями развития систем, основанных на тайне образа являются три типа биометрических технологий, построенных на анализе индивидуальных особенностей [3-5]: рукописного почерка; голоса; клавиатурного почерка.

Эти типы биометрических технологий имеют недостаточную стойкость при аутентификации личности на открытом биометрическом образе.

Необходимо подчеркнуть, что существенное снижение вероятности ошибки второго рода (пропуска «чужого») достигается за счет отсутствия у злоумышленника информации о воспроизводимом слове-пароле и о характерной для почерка человека графики и динамики при воспроизведении пароля [4].

Высоконадежная биометрическая аутентификация пользователей возможна только тогда, когда биометрические механизмы надежно сопряжены с криптографическими механизмами аутентификации. При совместном описании биометрических и криптографических механизмов возникает проблема согласования понятийного аппарата двух различных предметных областей. На данный момент один и тот же термин в «биометрии» и «защите информации», даже при полном языковом тождестве, имеют разное смысловое наполнение.

Одним из путей решения этой задачи является объединение терминов «биометрии» и «защиты информации», а также введение недостающих терминов в эти две предметные области, через использование более общего терминологического аппарата «теории информации».

В настоящее время идет активная работа по созданию системы международных биометрических стандартов. Для этой цели в ISO/IEC образован специальный подкомитет JTC1 SC37, отвечающий только за создание новых международных биометрических стандартов. В ближайшее время ISO/IEC JTC1 SC37 предполагает подготовить и принять порядка 20 международных биометрических стандартов. ГОСТ Р ТК355 ПК7, соответственно, начал работы по гармонизации для России и Казахстана первых биометрических стандартов [2].

Одним их основных понятий теории защиты информации является уровень защищенности, обеспечиваемый тем или иным механизмом защиты. Для примера, рассмотрим криптографический механизм защиты информации, построенный на алгоритме симметричного шифрования с длиной ключа 256 бит. Для измерения уровня защищенности по теории информации следует построить некоторый функционал вероятности преодоления этой защиты. Определим этот функционал следующим образом:

$$J_2 = -\log_2(P_2), \quad (1)$$

где J_2 – уровень защищенности, измеряемый в битах (длина эквивалентного симметричного двоичного ключа или логарифмическая мера числа возможных состояний эквивалентного ключевого поля), P_2 – вероятность преодоления защиты с первой попытки или вероятность удачи атаки случайного подбора ключа с первой попытки.

Как уже было отмечено, существует 3 основных технологии, основанных на тайне образа: рукописный почерк, голос, клавиатурный почерк. Каждая из них имеет разный уровень стойкости, которая в свою очередь зависит от совокупности информативности как самого статического образа (парольной фразы), так и динамических характеристик пользователя (динамики подписи, голоса, клавиатурного рисунка) [5].

Из перечисленных выше трех типов наиболее надежной является технология аутентификации личности по особенностям рукописного почерка. Это следствие того, что сохранить в тайне рукописно воспроизводимое слово-пароль (парольную фразу) много проще, чем сохранить в тайне аналогичную фразу, воспроизводимую голосом.

В свою очередь, данные системы имеют низкую стоимость оборудования, так как они могут использовать стандартные средства ввода рукописной графики. На сегодня многие карманные компьютеры имеют средства рукописного ввода в виде сенсорного экрана. Для настольных компьютеров могут быть использованы графические планшеты. Стоимость графического планшета EasyPainer составляет в России порядка 20 долл., что и послужило основной причиной ориентации на них отечественных производителей устройств биометрической аутентификации [6].

Реальные характеристики биометрических систем при работе с конкретными пользователями могут отличаться от среднестатистических на десятки порядков. Поэтому возникает необходимость отойти от абстрактного понятия «среднестатистический пользователь» и перейти к оценке стойкости, а соответственно информативности образа конкретного пользователя системы.

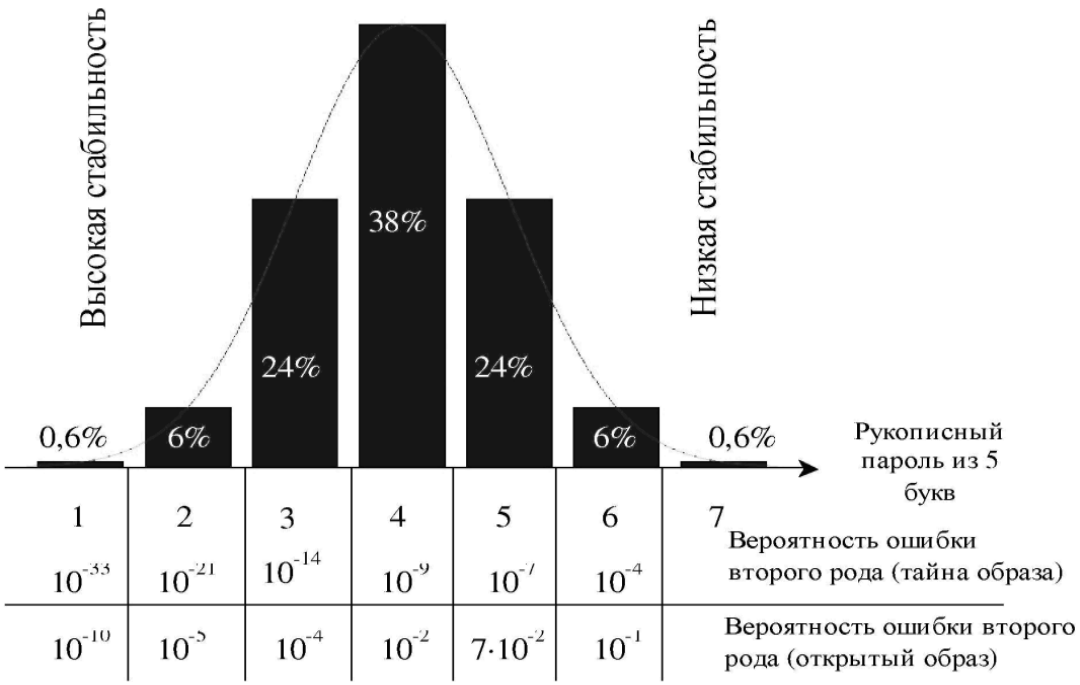

Рисунок 1 - Стойкость классов стабильности рукописного ввода

по отношению к атакам подбора

Статистические исследования системы «Нейрокриптон» показали, что всех людей можно разделить на 7 классов [6,7].

Каждый класс обладает различной стабильностью почерка, которая несколько зависит от парольного слова. То есть, пользователь при изменении его почерка может перейти на один класс ниже или выше, однако переход на 2 класса вверх и вниз возможен, но затруднен. Стойкость системы к атакам подбора существенно зависит от класса, к которому система отнесла пользователя. На рисунке 1 приведены процентные соотношения людей в каждом классе и стойкость классов по отношению к атакам подбора при условиях известного рукописного слова и неизвестного рукописного слова.

Наиболее стабильный класс пользователей при сохранении в тайне биометрического образа имеет вероятность ошибки второго рода на уровне 10^{-33}. Самый нестабильный седьмой класс пользователей вообще не может быть однозначно опознан системой. Среднестатистический пользователь имеет вероятность ошибки второго рода на уровне 10^{-9}. Получается, что люди с уникальным и стабильным почерком имеют вероятность ошибки второго рода на 24 порядка меньше, чем среднестатистический пользователь.

Системы аутентификации по голосовому образу, как и любые биометрические технологии, основанные полностью или частично на динамических параметрах пользователя, также могут имеют различную стойкость вследствии нестабильности этих параметров.

Для голосовых паролей прослеживается похожая зависимость стойкости, а следовательно и информативности от принадлежности к определенному классу стабильности. Данные приведены на рисунке 2.

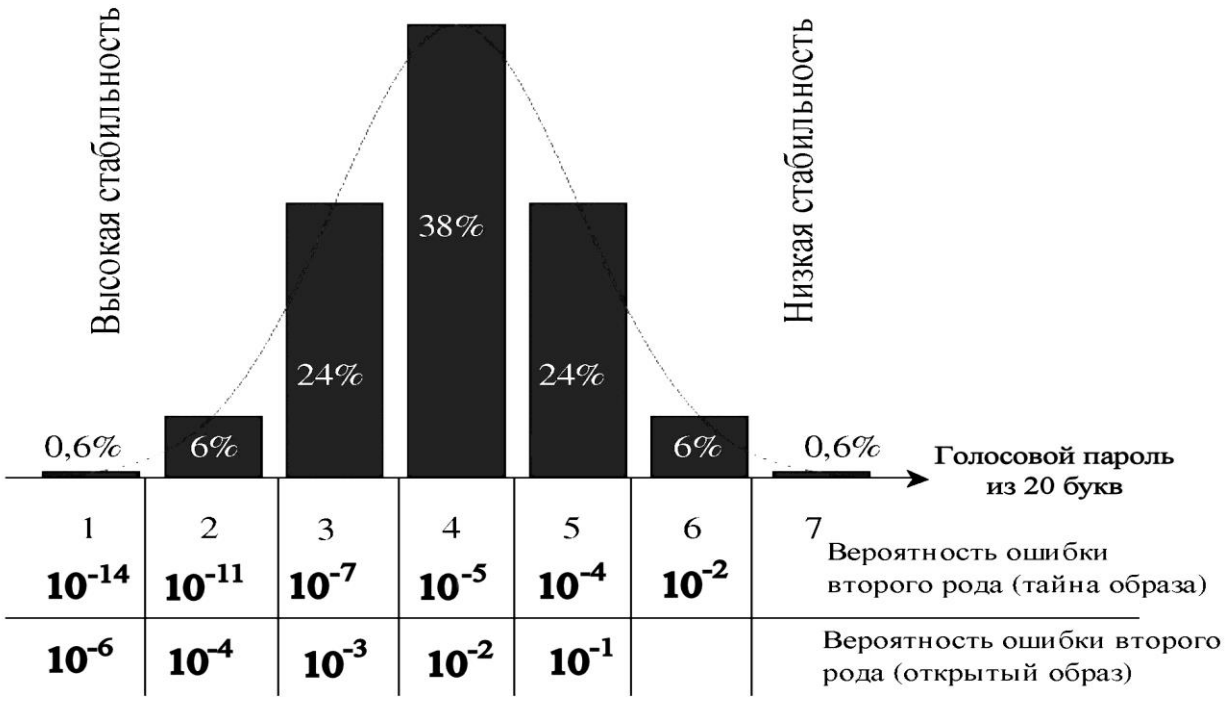

Рисунок 2 - Стойкость классов стабильности голосового ввода по отношению к атакам подбора

На данном графике приведены значения стойкости для парольной фразы «Невероятно сильный мороз», состоящий из 20 букв, по причине того, что голосовые пароли обладают существенно меньшей информативностью по сравнению с рукописными. В то же время это не является существенным недостатком, так как проговорить длинную фразу существенно проще, чем воспроизвести её написание, особенно для пользователей, входящих в группы с высокой нестабильностью (выше среднего).

Таким образом, стойкость системы во многом определяется индивидуальными характеристиками самого пользователя. Ошибка в определении класса может привести к завышению или занижению стойкости системы на несколько порядков. Необходимо использовать специальные нейросетевые механизмы для корректного и достоверного определения класса пользователя по его реальным биометрическим параметрам.

ЛИТЕРАТУРА

[1] Болл Руд и др. Руководство по биометрии. – М.: Техносфера, 2007.

[3] ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»

[3] Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во Пенз. гос. ун-та, 2000. – 188 с.

[4] Ахметов Б.С., Волчихин В.И., Иванов А.И., Малыгин А.Ю. Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации. –Казахстан, Алматы, КазНТУ им. Сатпаева, 2013 г.–152 с.

[5] Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Книга 15, серии «Нейрокомпьютеры и их применение». – М.: Радиотехника 2004. – 144 с.

[6] Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. – Пенза: Изд-во Пенз.гос.ун-та, 2005. – 273 с.

[7] Малыгин А.Ю. и др. Нейросетевое преобразование биометрического образа человека в код его личного криптографического ключа. Монография. – Москва, Радиотехника (ИПРЖ) книга №29 научной серии «Нейрокомпьютеры и их применение», 2008. – 87 с.