МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Крымский федеральный университет имени В.И. Вернадского»

ИНСТИТУТ ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА БИЗНЕС-ИНФОРМАТИКИ И МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

II Международная научно-практическая конференция

«Проблемы информационной безопасности»

25-27 февраля 2016

Симферополь — Гурзуф

Проблемы информационной безопасности: сборник научных трудов II Международной научно-практической конференции, Гурзуф, 25-27 февраля 2016 / Под ред. д.т.н., профессора О.В. Бойченко. — Саки: ИП Бровко А.А., 2016. — 256 с.

Комитет конференции:

Председатель:
Бойченко Олег Валерьевич
д.т.н., профессор

Члены комитета:
Апатова Н. В., д.э.н., д.п.н., профессор
Герасимова С. В., д.э.н., профессор
Климчук С. В., д.э.н., профессор
Пенькова И. В., д.э.н., профессор
Цёхла С. Ю., д.э.н., профессор
Сигал А. В., д.э.н., доцент
Королёв О. Л., к.э.н., доцент
Иванов С. В., к.ф.-м.н., доцент
Акинина Л. Н., ст. преподаватель
Бакуменко М. А., ст. преподаватель

Подписано в печать 15.02.2016 г.
Формат 60x90 $^1/_8$. Бумага офсетная. Гарнитура Times New Roman.
Усл. п.л. 30,68. Количество экз. 150

Напечатано в ИП Бровко А.А.
296500 г. Саки, ул. Тимирязева, 30

СЕКЦИЯ 8.
ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР, ПОЛЬЗОВАТЕЛЕЙ, ИХ ДАННЫХ И ИНТЕРЕСОВ

ысокий уровень применяемых технологий, и тесные связи между контрагентами, снованные на долгосрочных договорных отношениях, и публичность договорных тношений, вызывающая необходимость применения типовых форм гражданско-равовых договоров, и присутствие на рынке крупных корпоративных клиентов, пособных создать развитые информационные системы и вывести отрасль связи на ервое место в сфере развития новых форм документооборота [1].

Из всего вышесказанного можно сделать вывод, что лица, использующие ЭЦП, щищены от подделок документов, т.к. подобрать закрытый ключ к подписи отребуется очень много времени. Таким образом, основными преимуществами ЭП вляются: экономия времени на совершение сделки, безопасность и надежность в спользовании и хранении. Но, исходя из слабой законодательной базы в нашей стране, ожно говорить об отсутствии доверия со стороны граждан РФ столь инновационным пособам заключения сделок. Кроме этого, информация, которая содержится в лектронных документах, требует определенной защиты от каких-либо есанкционированных изменений. Если же ужесточить законодательство в данной фере, то на наш взгляд, в скором времени большинство позабудет что такое обственноручное заключение сделок.

Литература:

1. Батянов М.В., Лобачев В.В. Электронная цифровая подпись: проблемы правового применения: Материалы XI конференции представителей региональных научно-образовательных сетей RELARN-2004. - [Электронный ресурс]. - Режим доступа: www.ict.edu.ru/vconf/index.php.
2. Корелов С.В., Балыбердин А.В. Организация юридически значимого электронного документооборота с использованием электронной цифровой подписи: Методическое пособие / С.В. Корелов, А.В. Балыбердин; ННГУ. – Нижний Новгород, 2010. – 44 с.
3. Об электронной подписи : [федер. закон № 63-ФЗ от 6 апр. 2011 г.] // Рос. газ. – 2011. – 8 апр. – 18 полос.

УДК 004.056.5

Гончаров Сергей Михайлович
к.ф.-м.н., доцент
Боршевников Алексей Евгеньевич
ассистент
Кафедра информационной безопасности
ФГАОУ ВПО «Дальневосточный федеральный университет»
Владивосток, Россия

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Вопросы обеспечения безопасности являются важными для многих областей современного общества. С развитием общества появляются новые технологии для решения указанных вопросов. Одним из путей решения является процедура биометрической аутентификации. Требования к уровню безопасности, обеспечиваемому такой процедурой, будут различаться в зависимости от объекта, на котором необходимо обеспечить аутентификацию пользователей. Для некоторых объектов необходимо использовать средства высоконадежной биометрической аутентификации.

Согласно ГОСТ Р 52633.0-2006 под высоконадежной биометрической аутентификацией понимается биометрическая аутентификация с приемлемой вероятностью ошибок первого рода (т.е. отказа системы аутентификации при обработки данных легитимного пользователя) и гарантированно малой вероятностью ошибок второго рода (т.е. срабатывания системы аутентификации при обработке данных злоумышленника), сопоставимой по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора [1].

Примером объектов, на которых необходимо обеспечить высокий уровень безопасности за счет использования процедуры высоконадежной биометрической аутентификации, могут выступить критически важные объекты [2].

Еще одним примером задачи, в которой необходимо обеспечить высокий уровень безопасности, является задача идентификации пользователя в процессе дистанционного обучения. Эта задача очень актуальна в дистанционном обучении. Перед дистанционным обучением ставится цель высококачественной подготовки специалистов без очного взаимодействия с преподавателем. Однако возникает проблема при проведении промежуточного или итогового контроля, заключающаяся в том, что необходимо с достаточно большой степенью достоверности убедиться в том, что данные виды контроля проходит обучающийся, который должен их проходить, а не третье лицо. Однако подобную технологию не целесообразно использовать для контроля написания работы в текущее время, так как это требует дополнительных усилий, которые будут отвлекать пользователя от сдачи аттестационной работы. Поэтому целесообразно применять для всего процесса прохождения аттестации двухфакторную аутентификацию. Можно предложить следующую схему аутентификации пользователей при прохождении аттестации при дистанционной форме обучения:

1. Пользователь регистрируется в системе и предоставляет необходимые биометрические данные;
2. Для начала прохождения аттестации пользователь проходит идентификацию с помощью средств высоконадежной биометрической аутентификации. В случае прохождения данной процедуры пользователю предоставляется доступ к заданиям. Если пользователь не прошел аутентификацию, то доступ не предоставляется;
3. Во время прохождения аттестации в случайный момент времени с помощью веб-камеры делается снимок изображения лица пользователя и сравнивается с предоставленными на этапе регистрации пользователем данными. В случае соответствия снятых данных предоставленным пользователь продолжает проходить аттестацию, в противном случае аттестация прерывается.

Опишем процедуру высоконадежной биометрической аутентификации. В общем случае процедура высоконадежной биометрической аутентификации заключается в восстановлении из нечетких биометрических данных с использованием специально сгенерированных данных некоторой фиксированной битовой строки (криптографический ключ, код доступа, пароль). Основным преимуществом систем, основанных на описанном методе, является то, что вся аутентифицирующая информация не хранится в открытом виде, а хранится в виде некоторого хешированного значения. Это уменьшает размеры базы данных, используемой для аутентификации, а также позволяет обезопасить биометрические данные от компрометации.

В настоящий момент в мире на практике используются два подхода к реализации технологии высоконадежной биометрической аутентификации:

1. Подход, основанный на использовании "нечетких" контейнеров и "нечеткой" математики;
2. Подход, основанный на использовании аппарата больших и сверхбольших нейронных сетей (нейросетевые преобразователи "Биометрия - код доступа").

По данным открытых источников характеристики (вероятность ошибки первого рода, вероятность ошибки второго рода) нейросетевых преобразователей "Биометрия - код доступа" выше, чем характеристики биометрических систем, использующих "нечеткие" экстракторы [2]. Преимуществом "нечетких" экстракторов является их возможность использования для большинства видов биометрических характеристик, тогда как для нейросетевых преобразователей подробно описаны и изучены системы на основе рукописного почерка.

Одним из перспективных направлений исследований является разработка технологии высоконадежной биометрической аутентификации на основе электроэнцефалограммы (ЭЭГ). Использование ЭЭГ в качестве биометрической характеристики имеет следующее преимущество - ЭЭГ сложно снять незаметно для

пользователя, а также ее трудно подделать в силу сложности самой природы сигнала ЭЭГ.

В работе [3] в качестве биометрической характеристики, используемой в нейросетевом преобразователе, брался сигнал ЭЭГ под воздействием внешней зрительной стимуляции. Предварительные расчеты дали вероятность ошибки 2-го рода ниже, чем 10^{-12}.

Отдельный интерес представляют системы без внешней стимуляции. Проводились исследования на основе ЭЭГ, возникающей при специфическом движении глаз с закрытыми веками. Для выделения потенциала движения мышц глаз было решено провести следующий эксперимент. Для упрощения проведения эксперимента использовалась звуковая стимуляция метрономом, с интервалом 2 секунды. Запись данных производилась в течение 8 секунд. На каждый удар метронома испытуемый производил одно из движений алфавита 1 (движение влево, вправо, вверх, вниз) или алфавита 2 (движение влево, вправо, влево-вправо, вверх, вниз, вверх-вниз, по кругу). Последовательность движений составляет пароль.

Опишем структуру и принцип работы нейросетевого преобразователя "Биометрия - код доступа". Для обработки полученных данных в качестве структуры преобразователя выбрана двухслойная нейронная сеть с сигмоидальными передаточными функциями. Для обучения выбрана стандартная процедура обучения нейросетевых преобразователей "Биометрия - код доступа", описанная в стандарте ГОСТ Р 52633.5-2011 [4]. Для обучения необходимо сформировать базу электроэнцефалограмм при воздействии стимуляции образов "Чужой", т.е. образов злоумышленника, для которых нейронная сеть будет выдавать случайный криптографический ключ. Данную базу можно использовать для последующих процессов обучения преобразователя. Также необходимо сформировать базу электроэнцефалограмм образов "Свой" - пользователя, который будет считаться легитимным. Данную базу необходимо удалить сразу после обучения преобразователя, в целях предотвращения её кражи и использования для компрометации секретного ключа. Результатом выполнения данной процедуры будут являться весовые коэффициенты нейронной сети:

$$\overline{w_i} = \{w_{ij}\}, 1 \le i \le I, 1 \le j \le J,$$

$$\overline{W} = \{W_k\}, 1 \le k \le K,$$

где $\overline{w_i}$ – вектор весовых коэффициентов первого слоя нейронной сети, соответствующий вектору биометрических данных $\overline{a_i}$; $\overline{W}$ – вектор весовых коэффициентов второго слоя нейронной сети; K – количество нейронов первого слоя.

Нейроны первого и второго слоя сходны по строению, но имеют различие в обрабатываемых данных и получаемых результатах. Для описания работы первого слоя введем следующую величину:

$$v_i = \overline{a_i} \cdot \overline{w_i}, 1 \le i \le I.$$

Это нормированная величина, которая подается на входы сумматоров с электрода i. Составим вектор таких значений:

$$\overline{v} = \{v_i\}, 1 \le i \le I.$$

Работу каждого нейрона первого слоя можно описать следующим образом:

$$x_{1,k} = \overline{v} \cdot \overline{net_k},$$

$$\overline{net_k} = \{\Delta_i\}, 1 \le i \le I,$$

$$y_{1,k} = \frac{2}{1 + e^{x_{1,k}}} - 1,$$

$$t_k = f_1(y_{1,k}) = \begin{cases} 1, y_{1,k} \ge 0 \\ -1, y_{1,k} < 0 \end{cases}, 1 \le k \le K,$$

где $x_{1,k}$ – это результат работы сумматора нейрона k первого слоя; $\overline{net}_k$ - вектор связей нейрона k; Δ_i – коэффициент использования данных электрода i в нейроне. Если электрод используется в данном нейроне, то $\Delta_i = 1$ и $\Delta_i = 0$ в противном случае; $y_{1,k}$ – передаточная функция первого слоя нейронной сети; $f_1(y_{1,k})$ – решающее правило для нейрона первого слоя.

Используемые в сумматорах нейрона вектора нормированных биометрических данных определяются следующим образом. В любом сумматоре обязательно используется один из нескольких векторов, соответствующих векторам данных, характеризующим наиболее сильный потенциал движения глаз. Для оставшихся входов сумматора используются не использованные вектора нормированных биометрических данных.

Каждый нейрон второго слоя можно описать следующим образом:

$$x_{2,l} = \sum_{k=1}^{K} W_k t_k \Delta_l \,, 1 \le k \le K \,,$$

$$y_{2,l} = \frac{2}{1+e^{x_{2,l}}} - 1 \,,$$

$$k_l = f_2(y_{2,l}) = \begin{cases} 1, y_{2,l} \ge 0 \\ 0, y_{2,l} < 0 \end{cases}, 1 \le l \le L \,,$$

где $x_{2,l}$ – это результат работы сумматора нейрона второго слоя; Δ_l – коэффициент использования компонента t_k в нейроне. Если t_k используется в данном нейроне, то $\Delta_l = 1$ и $\Delta_l = 0$ в противном случае; $y_{2,l}$ – передаточная функция второго слоя нейронной сети; $f_2(y_{2,l})$ – решающее правило для нейрона второго слоя; L - длина восстанавливаемого криптографического ключа.

Используемые в сумматорах нейрона выходы первого слоя определяются согласно процедуре, описанной в ГОСТ Р 52633.5-2011 [4].

Результат работы каждого нейрона второго слоя k_l является битом восстанавливаемого секретного криптографического ключа.

Во всех опытах по восстановлению ключа легитимным пользователем вырабатываемый секретный ключ размером 256 бит всегда совпадал с истинным. Даже в случае, когда злоумышленник угадывает "мысленный пароль", минимальное расстояние Хэмминга (количество ошибок) до ключа легитимного пользователя было равно 15. При генерации злоумышленником ошибочного «мысленного пароля» усредненное расстояние Хэмминга до истинного ключа заметно выше.

Результаты исследования по получению злоумышленником секретного ключа размером 256 бит с помощью нейросетевого преобразователя при условиях знания пароля приведены в таблице 1. H_7 - расстояние Хэмминга при использовании алфавита «мысленных образов», состоящего из 7 символов.

Номер пользователя	H_7
1	136
2	138
3	47
4	20
5	143
6	15
7	88
8	50
9	144

Таблица 1. Расстояние Хэмминга до секретного ключа пользователя в случае знания злоумышленником пароля