Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 9, Пенза-2014, с. 67-69 (http://www.pniei.penza.ru/RV-conf/T9/C16)

БЕЗОПАСНОЕ МАССОВОЕ ВЗАИМОДЕЙСТВИЕ ГРАЖДАН С ЭЛЕКТРОННЫМ ПРАВИТЕЛЬСТВОМ

Ефимов О.В. (Пенза)

В настоящее время идут активные процессы информатизации современного общества. Одним из ярких и ощутимых процессов является декларирование всеми государствами намерения создания электронного правительства.

Электронное правительство России - это информационный ресурс высокого доверия, созданный государственными структурами РФ:

- Пенсионным фондом РФ;
- Служба социального страхования;
- Налоговой инспекцией;
- Федеральной службой судебных приставов;
- Федеральная служба исполнения наказаний;
- Федеральная служба по контролю за оборотом наркотиков;
- Федеральная миграционная служба;
- Федеральная таможенная служба;
- Министерство обороны РФ;
- Министерство внутренних дел РФ;
- МЧС РФ;
- ГИБДД;
- ……:

Электронное правительство субъектов России – это электронные ресурсы созданные правительствами регионов, областей, городов, поселений. Эти ресурсы формируются региональными органами самоуправления территорий:

- Областей;
- Районов;
- Городов;
- Поселений.

Перечисленные выше государственные электронные ресурсы являются ресурсами высокого доверия. То есть при взаимодействии с ресурсами электронного правительства гражданин должен быть уверен в том, что он имеет дело именно с представителями государства. С другой стороны государственные служащие должны быть уверены в том, что они взаимодействуют именно с тем гражданином, который имеет все права без ограничений и действительно является тем человеком, чье имя использовано для запроса.

В настоящее время взаимодействие граждан РФ с государственным службами и муниципальными образованиями осуществляется через электронные кабинеты. Например, каждый из граждан РФ может завести для себя личный кабинет с разделом Пенсионного фонда РФ на сайте государственные слуги (https://www.gosuslugi.ru). Доступ к ресурсу осуществляется при вводе пароля длинной 8 и более символов.

К сожалению, такой способ доступа к личной информации в своем электронном кабинете не безопасен. Люди стараются использовать короткие легко запоминаемые пароли (слабые пароли). Длинные плохо запоминаемые пароли из случайных знаков мало кто использует. Особенно это характерно для пожилых

людей, которые вообще стараются не пользоваться личными электронными кабинетами.

Для того, что бы повысить уровень защиты электронных кабинетов необходимо использовать стойкие к атакам подбора длинные пароли, максимально возможной длины (32 случайных знака) при этом нужно избавить пользователей от необходимости запоминать такие длинные случайные пароли.

Это технологически возможно, если пользоваться технологий нейросетевого преобразования биометрии человека в длинный пароль доступа из 32 случайных символов как это показано на рисунке 1.

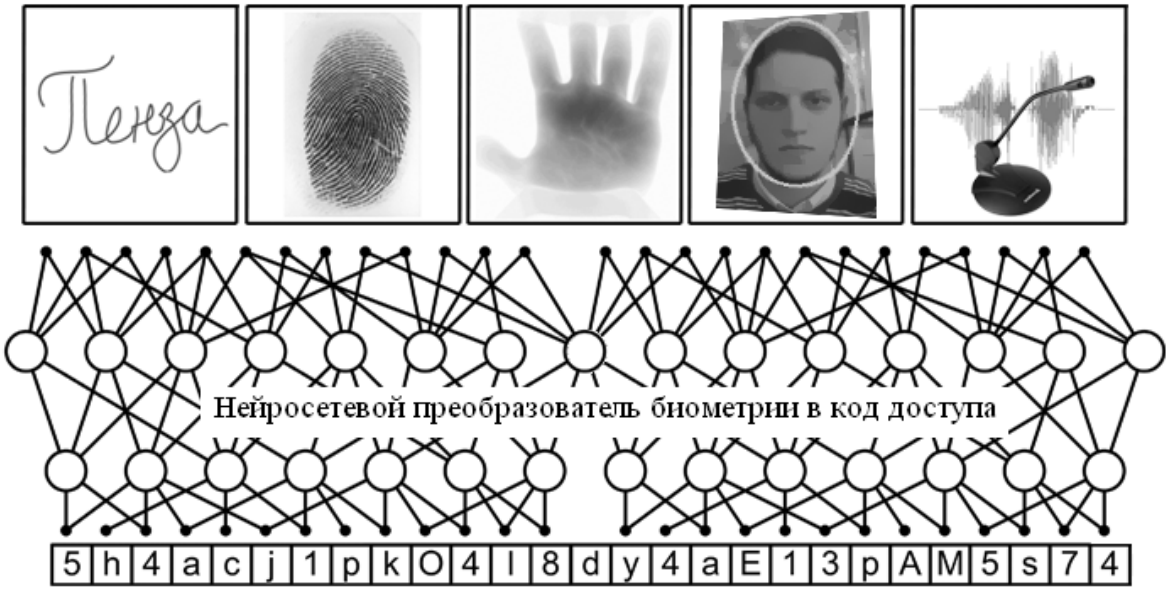

Рис. 1. Обученная нейронная сеть способна преобразовывать нечеткие биометрические данные в длинный код пароля доступа

В России разработаны отечественные технологии нейросетевого преобразования образов в длинный код пароля доступа. Как исходная информация доступа могут быть использованы:

- простые, легко запоминаемые рукописные пароли доступа, вводимые с чувствительного экрана планшетного компьютера или с графического планшета;
- голосовые пароли, произнесенные в микрофон компьютера или планшета;
- отпечатки пальца;
- веб-камеры компьютера;
- рисунок кровеносных сосудов ладони (используется USB сканер).

По новой технологии пользователю нет необходимости запоминать длинные случайные пароли доступа. Ему достаточно выбрать из списка нужный электронный кабинет и ввести свой биометрический образ доступа. При этом на выходе заранее обученной нейронной сети[1] появляется длинный пароль доступа из 32 случайных символов (см. рисунок 1).

Для использования предлагаемой технологии пользователю необходимо установить на свой компьютер программу и подключить устройство съема биометрических данных (если в компьютере нет чувствительного экрана, микрофона или веб-камеры).

[1] Обучение производится в течение нескольких секунд после предъявления пользователем нескольких примеров своего биометрического образа.

Для использования технологии никаких доработок серверной части не требуется!

Однако, учитывая, что переход на использование длинных надежных паролей произойдет не единовременно, на серверах целесообразно усилить меры безопасности, установив программное обеспечение, выявляющее слабые пароли по их хэш-функциям. Обнаружив слабый пароль администратор информационной безопасности должен оповестить пользователя об угрозе или запретить подкачку в слабо защищенный электронный кабинет чувствительной личной информации.

Дополнительно следует обеспечить пользователей тестерами стойкости, используемых ими паролей. Пользователь должен знать на сколько он рискует, применяя тот или иной пароль. Если пользователь решит использовать слабый пароль, например, «аааааааааааааааааааааааааааааа» средство должно предупредить его об опасности.

Комплекс средств безопасности (биометрические хранители паролей доступа, личные тестеры качества открытых паролей, серверные тестеры качества хэшированных паролей) должны обеспечить значительное повышение уровня информационной безопасности хранящейся в личных кабинетах электронного правительства РФ и электронных правительств субъектов РФ и муниципальных образований.

Естественно, что используемая нейросетевая технология должна быть безопасной, то есть она должна быть выполнена в соответствии с требованиями 7 отечественных стандартов (серии ГОСТ Р 52633.0-2006 ÷ ГОСТ Р 52633.6-2011), разработанных по заказу ФСТЭК России. Кроме того, предлагаемах технология рекомендована ФСБ России для защиты информационных ресурсов союзного государства.

Литература:

1. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
2. ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
3. ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
4. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
5. ГОСТ Р 52633.4-2012 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код».
6. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».
7. ГОСТ Р 52633.6-2013 «Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой».

Статью поступила 12.12.2014. Публикуется по положительной рецензии д.т.н. Малыгина А.Ю.