

**Системы биометрической аутентификации пользователя ПК по
клавиатурному почерку**

Бухтияров Борис Сергеевич, группа 11-Р,

Руководитель: Абашин В.Г.

Актуальность: В силу экономических причин для России наиболее дешевый путь ориентации биометрии на стандартные устройства ввода, видимо, является единственно приемлемым. Из-за экономических трудностей в течение последних лет российские разработчики биометрии не могли себе позволить дорогих устройств ввода и были вынуждены ориентироваться только на дешевые стандартные устройства.

Цель: Исследование системы биометрической аутентификации пользователя ПК по клавиатурному почерку, использующей в качестве меры близости образца подписи к биометрическому эталону.

Традиционные методы идентификации и аутентификации, основанные на использовании носимых идентификаторов, а также паролей и кодов доступа, имеют ряд существенных недостатков, связанных с тем, что для установления подлинности пользователя применяются атрибутивные и основанные на знаниях опознавательные характеристики. Указанный недостаток устраняется при использовании биометрических методов идентификации. Биометрические характеристики являются неотъемлемой частью человека и поэтому их невозможно забыть или потерять.

Важное место среди биометрических продуктов занимают устройства и программы, построенные на анализе динамических образов личности (аутентификация по динамике рукописной подписи, по клавиатурному почерку, по работе с компьютерной мышкой и т.п.).

Изучение клавиатурного почерка имеет давнюю историю. Еще в те времена, когда широко использовалась азбука Морзе и сообщения передавались с помощью телеграфа, предпринимались попытки определить индивидуальный клавиатурный почерк лица, посылающего сигнал. В принципе, надежное распознавание

пользователя по клавиатурному почерку возможно только при многопальцевом отработанном методе печатания. Если пользователь только начал работать с клавиатурой и печатает одним пальцем, то идентифицировать ввод информации очень сложно.

Одной из достаточно сложных задач, повседневно решаемых многими людьми, является быстрый ввод текстов с клавиатуры компьютера. Обычно быстрого клавиатурного ввода информации удастся достичь за счет использования всех пальцев обеих рук, при этом у каждого человека появляется свой уникальный клавиатурный почерк. Под этим понятием понимается система индивидуальных особенностей начертаний и динамики воспроизведения букв, слов и предложений на клавиатуре. Следует заметить, что применение способа идентификации по клавиатурному почерку целесообразно только по отношению к пользователям с достаточно длительным опытом работы с компьютером и сформировавшимся почерком работы на клавиатуре, т. е. к программистам, секретарям и т. д.

Классический статистический подход в распознавании пользователя по клавиатурному почерку при наборе ключевых слов выявил ряд интересных особенностей: существенна зависимость почерка от буквенных сочетаний в слове; существование глубоких связей между набором отдельных символов; наличие “задержек” при вводе символов. Кроме того, можно выявить и еще одну немаловажную особенность. Наиболее быстро абстрактный пользователь (т. е. некоторый образ усредненного пользователя) работает в середине рабочего дня (символическое название “День”), чуть медленнее утром и гораздо медленнее – вечером.

Существуют следующие алгоритмы распознавания:

– на основе геометрических методов распознавания, использующих различные меры близости предъявляемого вектора V к биометрическому эталону VC (мера Хэмминга, Евклидова мера и др.);

– на основе применения искусственных нейронных сетей (ИНС).

Методы, основанные на применении обучаемых нейронных сетей, потенциально обладают большей точностью, но им присущи две группы

принципиальных проблем: собственные проблемы искусственных нейронных сетей, связанные с возможностью возникновения неопределенно долгого процесса обучения, тупиков, состояния «паралича», а также проблемы, определяемые биометрической природой распознаваемых образов, главная из которых обучение - на всех возможных «чужих» пользователей (невозможность формирования представительной обучающей выборки для всех возможных «чужих»)

Геометрические методы распознавания наиболее просты, системы, их реализующие, обладают высоким быстродействием, однако ошибки аутентификации для таких систем могут оказаться неприемлемо большими. Это обусловлено тем, что используемые в геометрических методах меры близости фактически не учитывают конфигурацию областей распределения векторов биометрических параметров.

На практике особенности компьютерного почерка используют в качестве дополнительной степени защиты при вводе парольной фразы.

По мере того как компьютерные сети становятся распространенным явлением, проблема контроля приобретает все большую актуальность. Известно, что пароли часто крадут, к тому же людям свойственно использовать в качестве паролей информацию, которую им легко запомнить (номер своего телефона или автомобиля, имена детей и т.п.), что позволяет злоумышленнику зачастую просто догадаться и подобрать нужную комбинацию. Люди порой настолько беспечны, что оставляют на мониторе компьютера бумажку с паролями для входа в разные системы, на случай если код забудется. Но не будем останавливаться на технологии похищения паролей, скажем только, что в настоящее время хакерских приемов для этого существует великое множество.

Отпечаток пальца, радужка глаза и т.п. — каждый из этих методов имеет свою степень надежности и требует покупки определенного оборудования, а следовательно, и затрат. Преимущество защиты на основе распознавания клавиатурного почерка состоит в том, что этот способ не требует дополнительного оборудования и проверка может происходить в незаметном для пользователя, а значит и злоумышленника, режиме. Если хакер подобрал ваш пароль и пытается

войти в ваш компьютер, то система дает отказ по причине того, что пароль введен не с тем клавиатурным почерком.

Для оптимальной идентификации парольная фраза должна быть легко запоминаемой и содержать более 20 нажатий на клавиши. Однако системы, имеющиеся на рынке, работают и с более короткими парольными фразами (следует учесть, что в парольную фразу обычно входят и логин, и пароль). Биометрический эталон ввода получают на основе статистической обработки контролируемых параметров.

Одним из наиболее известных коммерческих продуктов в этой области является разработанный компанией Net Nanny Software технология BioPassword.

Вывод: использование данного метода позволяет выявлять несанкционированный доступ уже после процесса идентификации паролем или другим способом, защищает от подмены объекта и гарантирует аутентичность. Использование метода в паре с парольной или ключевой аутентификацией позволяет гибко настраивать систему безопасности, обеспечивая высокий уровень надежности. Наиболее перспективно применение данного метода при использовании удаленного рабочего места, в дистанционном обучении и в системах обнаружения несанкционированного доступа.

Литература

1. О.М. Лепёшкин, А.В. Скубицкий, Россия, г. Ставрополь, Ставропольский государственный университет [Электронный ресурс] / Режим доступа: <http://www.contrterror.tsure.ru/site/magazine11/03-11.htm>
2. Web-сервер журнала Компьютер Пресс [Электронный ресурс] / Режим доступа: <http://www.compress.ru/article.aspx?id=10007&iid=418#begin>
3. Непрерывная аутентификация методом клавиатурного почерка. [Электронный ресурс] / Режим доступа: <http://www.jurnal.org/articles/2009/inf5.html>