человеком. С одной стороны это имеет отрицательный эффект, так как люди все меньше общаются «вживую», при непосредственном контакте, но с другой стороны позволят общаться с человеком, который находится на другом конце света, а это согласитесь, имеет огромное значение.

Подведя итог можно сказать, что информационные технологии глубоко проникли в нашу жизнь, и современное общество уже не сможет в нынешнем виде существовать без них.

*Список использованных источников**:***

1. Официальный сайт Российской Государственной библиотеки для слепых [Электронный ресурс] – Режим доступа: www.rgbs.ru

2. http://www.rusarticles.com/internet-statya/znachenie-informacionnyx-texnologij-v-sovremennom-obshhestve-805378.html

Е.С. Федорова, РГППУ
гр. ИО-514
Руководитель: ст. преподаватель каф. СИС
С.В. Ченушкина

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПО КЛАВИАТУРНОМУ ПОДЧЕРКУ

В наше время всеобщей информатизации особую важность и значимость приобретают задачи защиты информации. Постоянно разрабатываются новые методы защиты, которые позволяют увеличивать надежность и стойкость систем, предназначенных для решения такого рода задач.

Среди задач защиты выделяются задачи аутентификации. И одними из наиболее перспективных и активно развивающихся сейчас методов являются методы биометрической аутентификации.

Среди плюсов биометрической аутентификации то, что характеристики каждого человека уникальны. У каждого свое неповторимое лицо, отпечатки пальцев, походка и пр. Не возникает проблема содержания в секрете пароля. Кроме того, биометрические характеристики всегда при человеке, он не может их «забыть» или потерять.

При рассмотрении любых систем распознавания важнейшими показателями таких систем являются вероятности ошибок системы. Если

система предназначена для разделения всех объектов на два класса, то для нее могут существовать две ошибки. Это так называемые ошибка первого рода (когда «своего» мы принимаем за «чужого») и ошибка второго рода (когда, наоборот, мы «чужого» принимаем за «своего»).

Вероятности ошибок первого и второго рода являются очень значимыми для систем распознавания. Именно значения вероятностей этих ошибок и определяют (в основном) качество функционирования системы.

В настоящее время активно развиваются методы биометрической аутентификации по статическим данным личности, как то: по двумерному изображению лица, трехмерному изображению лица, отпечаткам пальцев, радужной оболочке глаза, рисунку сосудов глазного дна, геометрии кисти руки, термографической картине лицевых артерий и вен, венам руки.

Так же существуют динамические методы биометрической аутентификации (аутентификация по особенностям голоса человека, по динамике рукописной подписи, по походке, по клавиатурному почерку, по работе с компьютерной мышкой, по характеру взаимодействия кисти руки и многое другое). Эти методы, во-первых, дают возможность изменять измеряемый образ. Так, человек может изменить контрольную фразу, которую вводит при аутентификации по клавиатурному почерку. Это делает такие системы предпочтительными при аутентификации личности по открытому каналу.

Рассмотрим систему аутентификации личности по клавиатурному почерку.

В свое время для идентификации телеграфистов, работавших с кодом Морзе, использовалось то обстоятельство, что у каждого телеграфиста при такой передаче информации вырабатывался свой собственный индивидуальный почерк.

Аналогично и для людей, постоянно набирающих тексты с клавиатуры. Каждый по-своему набирает текст. При этом можно идентифицировать пользователей по скорости набора, по ритмическим характеристикам набора; можно учитывать количество ошибок, их характер и т.п.

Возможность аутентифицировать клавиатурный почерк человека появляется при вводе в качестве пароля фразы, состоящей из достаточно большого количества букв. Система фиксирует времена нажатия клавиш и

интервалы между нажатиями и отпусканиями клавиш (контрольные параметры).

Скорость набора и контрольные параметры значительно зависят от того, сколько пальцев используется при наборе. При наборе одним пальцем одной руки клавиатурный почерк теряет свою уникальность. Это происходит из-за того, что при наборе несколькими пальцами интервалы между нажатиями зависят от характерных для каждого пользователя сочетаний движения пальцев рук и самих рук тоже. При наборе одним пальцем интервалы становятся пропорциональными временам нажатия клавиш.

При совершенствовании навыков работы с клавиатурой растет и индивидуальность набора каждого пользователя.

Установлено, что парольная фраза должна быть по длине не менее 20 символов. Причем при наборе этой фразы допустимы ошибки в 1-2 символах. Это ухудшает стойкость системы, но зато сильно уменьшает вероятность «ложной тревоги».

Можно выделит следующие преимущества аутентификации личности по клавиатурному почерку:

- дешева в реализации, т.к. для нее не нужно специализированное оборудования для измерения характеристик. Такую систему можно реализовать с помощью стандартной клавиатуры. Поэтому стоимость системы определяется в основном стоимостью программного обеспечения;
- возможность сделать биометрические образы тайными;
- идентификация очень удобна для пользователя: вроде бы он вводит обычный пароль, а на самом деле система точно определяет, имеет ли право сидящий за компьютером на доступ к информации.

Недостатком данной технологии является: временное изменение этого самого почерка у пользователей под влиянием стрессовых ситуаций. Что, в свою очередь, может привести к отказу в доступе человеку, имеющему на это право.

Технология идентификация по клавиатурному почерку имеет две разновидности:

- статичная - анализ указанных выше характеристик только в конкретных случаях (например, при наборе имени пользователя и пароля);
- непрерывная - контроль характеристик машинописи в течение всей работы на ПК.

Технология аутентификации личности по клавиатурному почерку не была протестирована для использования в достаточном количестве приложений, тем не менее наиболее вероятная область ее применения в будущем может быть контроль доступа к ПК, и контроль использования клавиатуры, например, в случае обращения к документам высокой степени секретности.

П.Ю. Цыганок, Д.С. Мальгин, РГППУ
гр. КТ-305
Руководитель: ст. преподаватель каф. СИС
Е.В. Болгарина

ЛЕГКО ЛИ СОВРЕМЕННОМУ ПОЛЬЗОВАТЕЛЮ ПЕРЕЙТИ НА LINUX?

Linux (GNU/Linux) - семейство операционных систем на основе ядра linux и собранных для библиотек и программ. Первая версия ядра была разработана в 1991 году финским студентом Линусом Торвальдом. Новые версии ядра linux разрабатывают он и многочисленные разработчики по всему миру.

На основе ядра Linux разработано множество операционных систем — Ubuntu, OpenSuse, Mandriva Linux, Fedora, Debian, Gentoo, Slackware и др. Опытные пользователи могут сами собрать свой дистрибутив операционной системы из исходных пакетов. В этой статье мы рассмотрим два популярных дистрибутива: Ubuntu 9.10 и Mandriva Linux 2010.

Рассмотрим причины перехода на Linux:

- Цена. Дистрибутивы Linux, в основном, бесплатны, хотя существуют и платные (оставаясь дешевле MS Windows).Операционную систему можно без проблем скачать из Интернета или заказать диск или бокс по почте. При приобретении платного дистрибутива, пользователь получает техническую поддержку.
- Свобода выбора. Существует множество разных версий дистрибутивов операционных систем: для начинающего пользователя, для "продвинутых" пользователей, для системных администраторов, для программистов и т.д. Выбор внешнего вида операционной системы (разные графические менеджеры), софта (в основном бесплатного).