Мазниченко Н.И.
ст. преподаватель
Национальный юридический университет
им. Ярослава Мудрого
Кафедра информатики и вычислительной техники
г. Харьков, Украина

ОГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ СИСТЕМ ИДЕНТИФИКАЦИИ

Создание единой централизованной системы безопасности является необходимым условием существования современной информационной инфраструктуры. Одним из основных и неотъемлемых элементов комплексной системы безопасности является подсистема управления доступом к информационным ресурсам. В последнее время в связи с увеличением угроз для компьютерной информации все больше внимания уделяется задачам совершенствования существующих и разработке новых средств защиты компьютерных систем от нежелательного доступа со стороны неавторизованных пользователей. Система идентификации является одним из ключевых элементов инфраструктуры защиты от несанкционированного доступа к какой-либо компьютерной системе [1]. Идентификация - это предъявление пользователем какого-либо уникального, свойственного только ему идентификатора (признака).

Сегодня существует несколько способов идентификации пользователей. У каждого из них есть свои преимущества и недостатки, поэтому каждому конкретному пользователю нужно самостоятельно выбирать, какой из способов реализовывать в собственных компьютерных системах.

Существуют следующие распространенные подходы к идентификации пользователей компьютерных систем:

1. Парольная идентификация. Суть ее сводится к следующему. Каждый зарегистрированный пользователь какой-либо компьютерной системы получает набор персональных реквизитов (чаще всего используются пары логин-пароль). Далее, при каждой попытке входа в систему, он должен указать свою информацию. Ну а поскольку она уникальна для каждого пользователя, то на основании ее система делает заключение о личности и идентифицирует ее.

Главное преимущество парольной идентификации - это простота реализации и использования. Кроме того, ввод парольной идентифи-

кации не требует никаких затрат: данный процесс реализован в большинстве программных продуктов.

Теперь перейдем к недостаткам. К сожалению, их много. И самый, пожалуй, главный - огромная зависимость надежности идентификации от самих пользователей, точнее, от избранных ими паролей. Дело в том, что большинство людей использует ненадежные ключевые слова, которые легко подбираются. Поэтому некоторые специалисты в области информационной безопасности советуют использовать длинные пароли, которые состоят из случайного соединения букв, цифр и различных символов [2].

2. Аппаратная (электронная) идентификация. Этот принцип идентификации основывается на определении личности пользователя по какому-либо предмету, ключу, что находится в его эксклюзивном использовании [3]. На данный момент наибольшее распространение получили два типа устройств: разнообразные карты (проксимити-карты, смарт-карты, магнитные карты и т.д.) и так называемые токены (token), подключаемые непосредственно к одному из портов компьютера.

Главным достоинством применения аппаратной идентификации является довольно высокая надежность. И действительно, в памяти токенов могут храниться ключи, подобрать которые достаточно сложно. Кроме того, в данных устройствах реализовано немало различных защитных механизмов.

Ну а теперь поговорим о недостатках аппаратной идентификации. Пожалуй, наиболее серьезной опасностью является возможность кражи злоумышленниками токенов или карт у зарегистрированных пользователей. Также они могут быть потеряны, переданы другому лицу, дублированы. Другой минус рассмотренной технологии - цена. Следует отметить, что в последнее время стоимость как самих электронных ключей, так и программного обеспечения, которое может работать с ними, заметно снизилась. Однако, для ввода в эксплуатацию такой системы идентификации потребуются некоторые вложения.

3. Биометрическая идентификация. Биометрия - это идентификация человека по уникальным, свойственным только ему биологическим признакам [4]. Можно сказать, что биометрические технологии изначально разрабатывались для точного установления личности человека, поэтому решение использовать их в области информационной безопасности выглядит вполне логичным.

Среди биометрических механизмов идентификации можно выделить такие:

- по статическим признакам - то, что практически не меняется со временем, начиная с рождения человека (физиологичные характеристики);
- по динамическим признакам - поведенческие характеристики, то есть те, которые построены на особенностях, характерных для подсознательных движений в процессе воссоздания какого-либо действия. Динамические признаки могут меняется со временем, но не резко, а постепенно.

Среди статических методов идентификации пользователя сегодня используются следующие: идентификация по отпечатку пальца, по расположению вен на ладони, по сетчатке глаза, по радужной оболочке глаза, по форме кисти руки, по форме лица.

Среди используемых динамических методов можно назвать следующие: идентификация по голосу, по почерку, по клавиатурному почерку.

При всем теоретическом многообразии биометрических методов тех, которые применяются на практике, немного. Чаще всего используют: распознавание по отпечатку пальца, по изображении лица (двухмерному или трехмерному) и по радужной оболочке или сетчатке глаза.

Главным преимуществом биометрических технологий является наивысшая надежность. И действительно, всем известно, что двух людей с одинаковыми отпечатками пальцев в природе просто не существует.

Основным недостатком биометрической идентификации является стоимость оборудования. Ведь для каждого компьютера необходимо приобрести собственный сканер. Хотя следует отметить, что в последнее время цены на биометрические устройства постоянно снижаются.

Пока что было рассмотрено три вида (или подхода) однофакторной идентификации пользователей компьютерных систем. То есть в рассмотренных системах для определения личности пользователя использовался только один фактор (одна характеристика). Однако подобные подходы сегодня нельзя назвать надежными. В последнее время получает распространение комплексная или многофакторная идентификация.

В системах комплексной идентификации для определения личности пользователя компьютерной системы применяется сразу несколько параметров [5]. Причем, комбинироваться эти факторы могут в произвольном порядке. Однако, наиболее часто сегодня используется

только одна пара: парольная защита и токен. В этом случае пользователь может не бояться подбора пароля злоумышленником (без электронного ключа пароль работать не будет), а также кражи токена (он не будет работать без пароля). Впрочем, в некоторых системах применяются максимально надежные процедуры идентификации, в которых одновременно используются пароли, токены и биометрические характеристики.

Внедрение комбинированных систем увеличивает количество идентификационных признаков и тем самым повышает безопасность компьютерных систем.

На основе анализа угроз информационной безопасности и существующих средств идентификации пользователей компьютерных систем можно уверенно сказать, что парольная защита на сегодняшний день является одним из самых распространенных способов защиты информации от несанкционированного доступа как в отдельных компьютерных системах, так и в сетях мирового масштаба. Однако без использования других механизмов пароль не может обеспечить серьезной защиты, достаточной для требований современности. Достаточно распространенными в качестве идентификаторов являются также разнообразные электронные ключи (токены, карты и т.д.). Хотя следует заметить, что в последнее время все большее распространение получают системы идентификации, которые используют биометрические характеристики человека при решении задачи доступа к компьютерным системам.

Таким образом, рассмотрев различные технологии идентификации можно сделать вывод, что в дальнейшем по мере роста вычислительных мощностей все более востребованным будет использование систем многофакторной идентификации, которая сочетает несколько подходов к решению задачи доступа к информационным ресурсам компьютерных систем, что, в свою очередь, позволяет значительно повысить надежность и защищенность данных систем.

Литература:

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004 г. – 384с.
2. Даклин Пол. Простые советы по более разумному выбору и использованию паролей / Пол Даклин. [Электронный ресурс]. Режим доступа: http://www.infosecurity.ru/_gazeta/content/060525/article01.shtml
3. Джхунян, В.Л. Электронная идентификация / В.Л. Джхунян,

В.Ф. Шаньгин. – М.: NT Press, 2004. – 695 с.
4. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
5. Шрамко В.Н. Комбинированные системы идентификации и аутентификации // PCWeek/RE. - 2004. - №45.

Sidorova M.G.
PhD,
Oles Honchar Dnipropetrovsk National University, Dnipropetrovsk, Ukraine

INFORMATION TECHNOLOGY OF CLUSTER ANALYSIS OF MONITORING FACILITIES WITH TIME-VARYING FEATURES

Recently, there has been a tendency to accumulation the large amounts of information in connection with the improvement of technology for recording and storing monitoring data. A problem of processing large volumes of data sets to identify hidden knowledge, laws, properties, trends has arisen.

Clustering is an important initial step in the data mining process, which is used to identify groups, hierarchical structures and patterns in the data set. The objective of cluster analysis is to part a data set into groups (clusters) so that the samples within the same cluster are more similar to each other than samples from different clusters. Using the clustering techniques allows us to understand the structure of multidimensional data; to simplify further processing using different methods of analysis for each cluster; reduce the original sample data, leaving the most typical representatives of each group; detect novelty, atypical objects that can not be attached to any of the classes; formulate or test hypotheses based on the results.

Time series analysis and clustering are the most important tasks of data mining. In recent years, more attention is paid to the unification of these areas, as the actual problem is the allocation of homogeneous groups of the time series for further analysis and prediction.

The purpose of this work is the creation the information technology of cluster analysis of monitoring results to define groups of objects by similarity of attributes as in every moment and in the time period of observation, and also the similarity of some attributes' change, evaluating the