УДК 004

РАЗРАБОТКА СИСТЕМЫ ИДЕНТИФИКАЦИИ/АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ АНАЛИЗА СУЩЕСТВУЮЩИХ СИСТЕМ

Вдовиченко А.О, студент гр. МРм-151, 2 курс
Научный руководитель: Ванеев О.Н., к.т.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

В современных информационных системах (ИС) обрабатывается большое количество различных данных. Зачастую это персональные данные (ПД), или любые другие данные, которые должны быть конфиденциальными, т.е должны быть известны только определенному кругу лиц (пользователям ИС или работникам организации где внедрена ИС). Для обеспечения конфиденциальности таких данных, в современных ИС предусмотрены системы защиты, включающие в себя механизмы идентификации и аутентификации пользователей. На сегодняшний день существуют следующие системы идентификации (аутентификации) пользователей.

Системы идентификации:

- Штрих - кодовая идентификация;
- Радиочастотная идентификация;
- Идентификации на основе карт с магнитной полосой;
- Биометрическая идентификация.

Системы аутентификации:

- Аутентификация по многоразовым паролям;
- Протокол аутентификации Kerberos;
- Протоколы аутентификации для удалённого доступа (PAP, CHAP, EAP, RADIUS, TACACS);
- Аутентификация на основе одноразовых паролей;
- Аутентификация по предъявлению цифрового сертификата;
- Использование смарт-карт и USB-ключей.

В рамках работы, для анализа мы будем использовать существующие системы идентификации, аутентификации, при этом более предпочтительными для анализа являются: биометрические механизмы идентификации, а также аутентификация по одноразовым и многоразовым паролям.

Такой выбор для анализа обусловлен тем, что зачастую такие механизмы защиты обеспечивают приемлемый уровень защищенности ИС, а также являются относительно недорогими.

Краткий обзор выбранных систем идентификации / аутентификации

Идентификация с помощью биометрических данных представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик.

Работа с биометрическими данными организована следующим образом: Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца, обычно не хранятся).

В дальнейшем для *идентификации* (и одновременно *аутентификации*) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Парольная аутентификация представляет собой метод аутентификации, основанный на том, что пользователю известна (I – Know) некоторая конфиденциальная информация-пароль, на основе которой пользователь получает доступ в систему.

Цель работы:

Изучить вышеуказанные методы идентификации и аутентификации, на основе анализа этих систем разработать более эффективный и упрощенный алгоритм распознавания пользователей.

Для достижения указанной цели в работе должны быть решены следующие задачи:

1.Анализ существующих систем идентификации/аутентификации пользователей

2.Разработка алгоритма идентификации/аутентификации на основе анализа существующих систем

3.Разработка алгоритма при помощи программных средств.

4.Теситрование алгоритма.

Пример реализации алгоритма упрощенной парольной аутентификации:

В классической ситуации, символьный пароль, придуманный заранее выдаётся администратором ИС или вводится пользователем, заносится в БД и сохраняется. Для входа в систему пользователю необходимо знать свою конкретную комбинацию символов – пароль. Детализация этого процесса представлена на диаграмме деятельности рис.1.

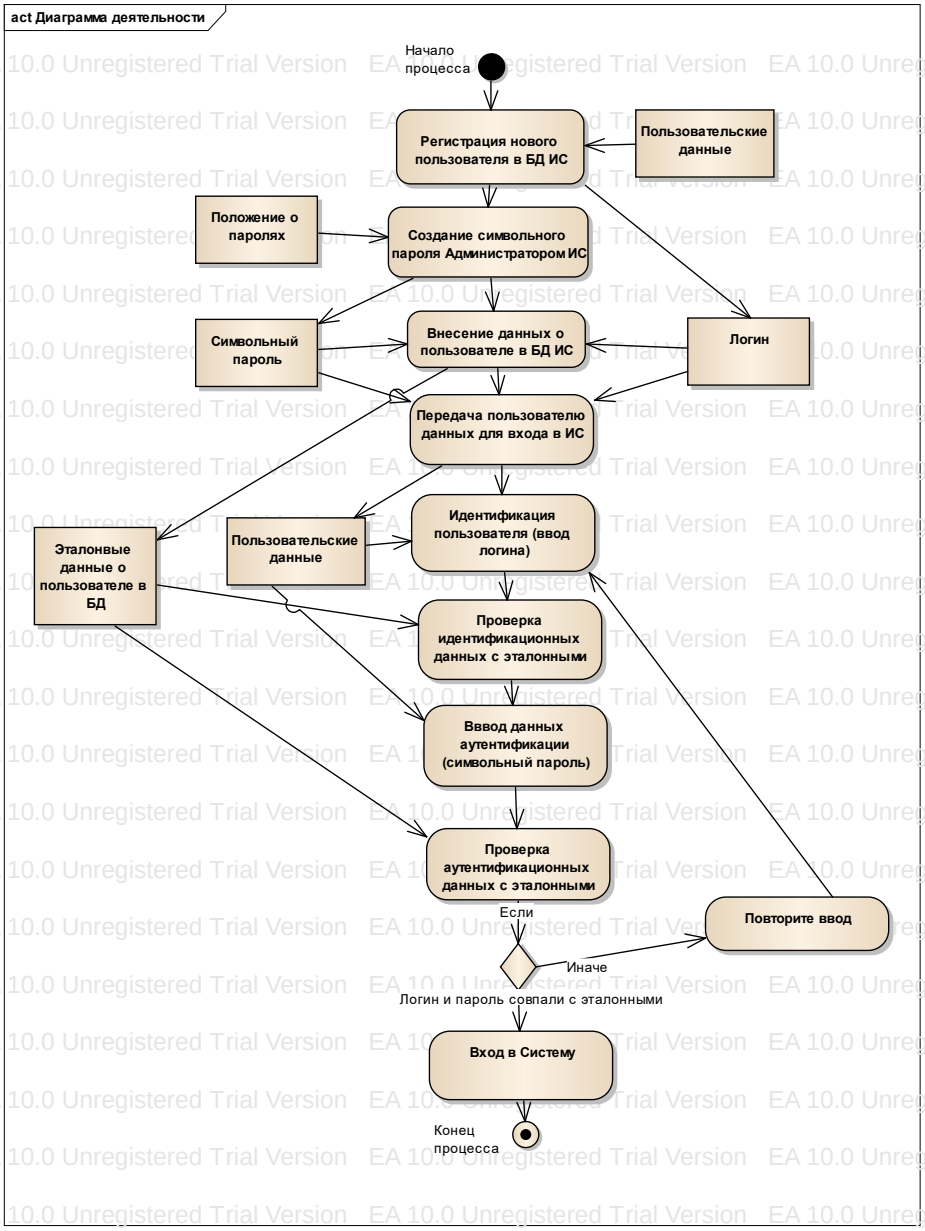

Рис.1 Диаграмма деятельности, отображающая процесс классической парольной аутентификации

Согласно разрабатываемому мной алгоритму, пароль будет генерироваться на основе введенной графической карты пользователя при регистрации. Для входа в систему пользователю необходимо будет ввести свой рисунок. Главным достоинством данного алгоритма является облегчение процесса хранения информации в памяти пользователя в наглядном виде: в виде графической карты, а не последовательности символов, которые человек склонен забывать и зачастую это приводит к неудобствам. На рис. 2 представлена диаграмма деятельности, отображающая процесс регистрации и входа в систему с использованием нового алгоритма.

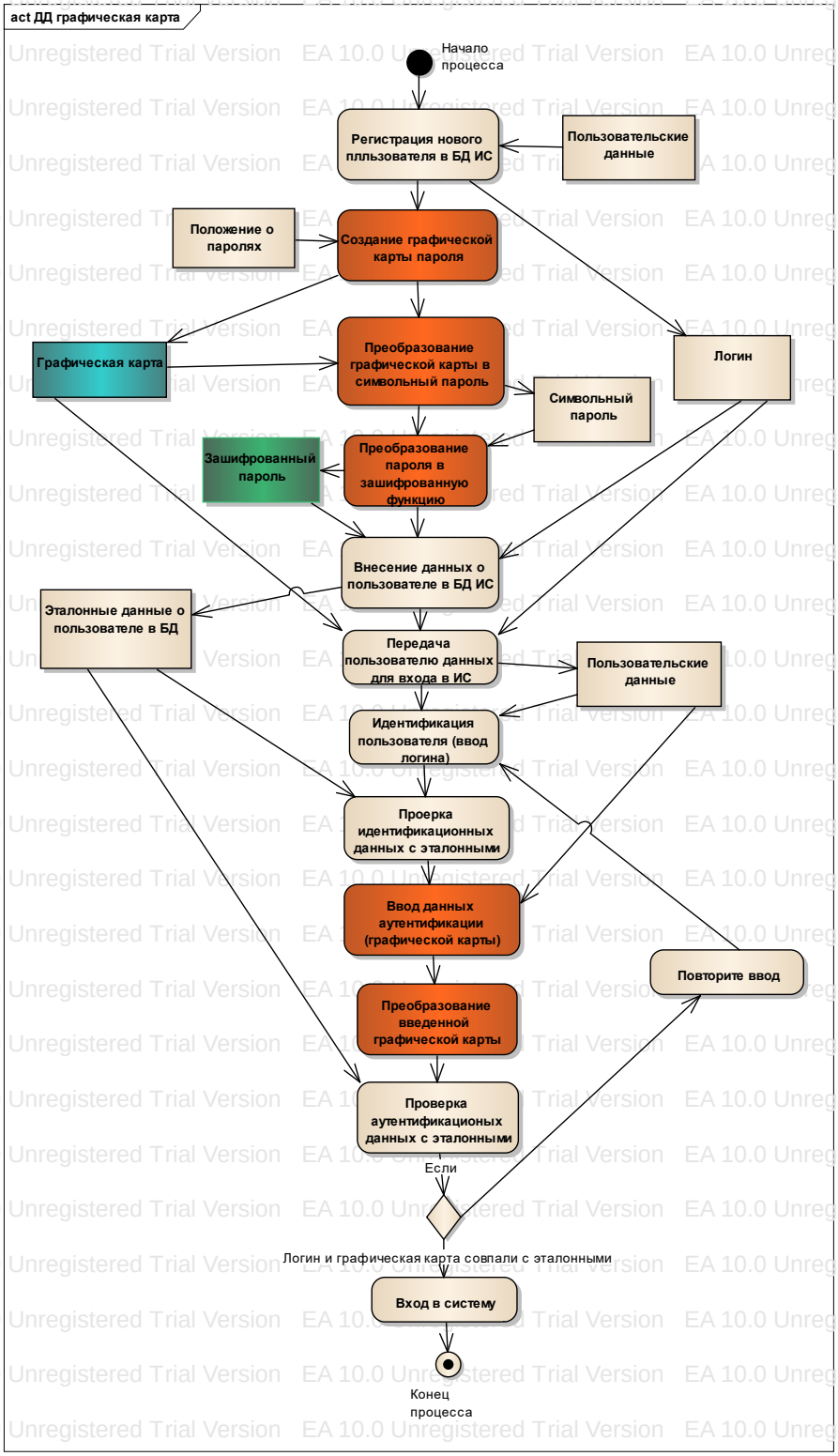

Рис.2 Диаграмма деятельности, отображающая процесс входа в ИС, с использованием графической карты

Используемые технологии для разработки:

1.MS SQL Sever 2008R2: Система управления реляционными базами данных, разработанная корпорацией Microsoft.

2.Visual Studio 2010 Ultimate: полнофункциональная интегрированная среда разработки (IDE) для приложений на ОС Windows, Web- и облачных приложений

Внедрение разрабатываемого алгоритма идентификации/аутентификации пользователей будет осуществляться в информационную систему обработки данных о пластиковых картах ОАО УРАЛСИБ. Это позволит повысить удобство обслуживания и уровень защиты данных от несанкционированного доступа.

Список литературы:

1.Материалы с сайта Википедия. [Электронный ресурс]. URL: http://ru.wikipedia.org/

2. Обзор технологий идентификации и аутентификации [Электронный ресурс]. URL: http://www.infosecurity.ru/cgi-bin/mart/arts.pl?a=_060920