А.А. ФОМИН,
А.А. ТРИФОНОВ

Обзор методов идентификации в информационных системах

УДК 004.056.53

Муромский институт (филиал) ФГБОУ ВО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых», г. Муром

В статье проведен обзор современных методов идентификации пользователей в информационных системах, рассмотрены области применения этих методов, их достоинства и недостатки.

Введение

Повсеместное внедрение информационных технологий и компьютерных сетей требует решения задач обеспечения информационной безопасности и защиты хранимой информации. Наиболее распространенным подходом является использование технологий разграничения доступа на основе идентификации и аутентификации пользователей [1].

Несовершенство некоторых широко применяемых подходов часто становится причиной несанкционированного доступа к информационному объекту и нарушения конфиденциальности. Развитие методов и систем управления доступом посредством идентификации является одним из приоритетных направлений развития информационных систем [2].

Классификация методов идентификации

По используемым средствам выделяют следующие методы идентификации пользователей [3]:

1. Метод, основанный на знании некоторой секретной информации – пароля.

2. Метод, основанный на использовании уникального предмета – жетона, электронной карточки и т.п.

3. Метод, основанный на измерении биометрических параметров человека – физиологических или поведенческих.

Парольная идентификация

В настоящее время данный метод идентификации является самым распространенным и популярным, ввиду понятности принципов работы и простоты реализации. Метод основан на вводе идентификатора и пароля с последующим их сравнением с эталонными значениями, хранящимися, как правило, в зашифрованном виде [4].

Парольная идентификация широко используется в информационных системах, операционных системах и иных сервисах. При правильном использовании паролей, они могут обеспечить приемлемый уровень безопасности. Однако, по совокупности характеристик, данный вид идентификации является самым слабым средством проверки подлинности [5].

К достоинствам метода относят:

1. привычность;
2. простота реализации;
3. дешевизна технологии.

К недостаткам относят:

1. частое отсутствие требований к сложности пароля;
2. возможность подбора и перехвата пароля;
3. Длительное время идентификации.

Повышение надежности парольной защиты может быть достигнуто за счет использования ряда мер:

1. наложения технических ограничений на пароль;
2. управления сроком действия паролей, и их периодической смены;
3. ограничения доступа к хранилищу паролей;
4. ограничения числа неудачных попыток ввода пароля;
5. обучения пользователей;
6. использования методов шифрования при передаче пароля.

Недостатки технологии парольной защиты ограничивают область ее применения авторизацией пользователей в информационных системах и получения доступа к ресурсам данной

системы [6]. Также возможно применение этой технологии для реализации простейших систем контроля и управления доступом.

Применение данной технологии в задачах автоматизации, например, производственных процессов (учет товаров, логистика, управление производством) невозможно из-за необходимости многократного ручного ввода кода, что существенно повышает вероятность ошибок. Для решения таких задач, в настоящее время используют иные методы, основанные на записи кода (пароля) на некотором материальном носителе, допускающем автоматическое считывание[7].

Штриховая кодовая идентификация

Штриховые коды получили широкое распространение в автоматических и автоматизированных системах ввода информации в целом ряде производственных областей[8].

Данная технология основана на обработке штрихового кода (последовательности светлых и темных полос различной ширины) специальными считывателями, которые распознают код, осуществляют заложенные методы контроля и передают код в информационную систему.

Различают два типа штриховых кодов: одномерные и двумерные.

Среди одномерных кодов выделяют два основных стандарта: американский UPC и европейский EAN [9]. Оба стандарта изначально предназначались для кодирования товаров, что определило их структуру и ограниченный объем кодируемой информации (до нескольких десятков символов). Такой код разбит на группы полей для указания кода страны производства, кода производителя, кода товара и контрольного числа. Однако, в штриховом коде можно записать любую цифровую последовательность (в некоторых случаях буквенно-цифровую), что позволяет использовать такие коды и для идентификации пользователей информационных систем.

В процессе развития технологии штрихового кодирования возникла необходимость кодирования большего объема информации, например, описания товара или сайта производителя. В итоге были разработаны двумерные коды, наиболее

распространенным из которых является QR-код [10]. QR-код позволяет закодировать значительно больший объем информации (более 2 Кб текста), что существенно расширяет спектр его применений.

К достоинствам применения штрих-кодовой идентификации относятся:

1. Максимальное снижение бумажного документооборота и количества ошибок при вводе информации.

2. Повышение скорости обслуживания клиентов.

3. Автоматизация основных технологических процессов товародвижения на всех этапах от производителя до конечного покупателя.

Основные недостаткам штрих-кодовой идентификации:

1. Данные идентификационной метки не могут дополняться.

2. Данные на метку заносятся медленно.

3. Данные на метке представлены в открытом виде и не защищают товары от подделок и краж.

4. Штрих-кодовые метки недолговечны, т.к. не защищены от пыли, сырости, грязи, механических воздействий.

Штриховые коды могут использоваться везде, где требуется быстрый и точный ввод информации в ИС:

1. маркировка товаров;

2. контроль состояния грузов;

3. получение информации об изготовлении продукции;

4. ввод данных в базы данных.

Для целей обеспечения безопасности и контроля доступа штриховые коды подходят слабо, поскольку не обеспечивают приемлемого уровня защиты, ввиду простоты считывания и подделки.

В последнее время штриховая кодовая идентификация вытесняется более перспективной технологией, основанной на радиочастотах [11].

Радиочастотная идентификация

Радиочастотная идентификация (RFID) – технология, позволяющая производить считывание и запись данных с помощью радиосигналов [12]. В ее основе лежит технология передачи с

помощью радиоволн информации, необходимой для распознавания объектов, на которых закреплены метки, несущие как идентификационную, так и пользовательскую информацию.

Радиочастотная технология развивает достоинства штриховой кодовой идентификации и исправляет практически все ее недостатки. В настоящее время данная технология внедряется во многие отрасли народного хозяйства, так как она позволяет получать информацию без прямого контакта. Дистанции, на которых может происходить считывание и запись информации, могут варьироваться от нескольких миллиметров до нескольких метров в зависимости от используемых технологий [13].

Система идентификации состоит из RFID-меток, которые однозначно идентифицируют объект, и считывающего устройства, позволяющего считывать данные с меток и преобразовывать их для дальнейшей обработки [14].

К достоинствам технологии относятся:

1. возможность перезаписи;
2. отсутствие необходимости в прямой видимости;
3. большое расстояние чтения;
4. поддержка чтения нескольких меток;
5. считывание данных метки при любом её расположении;
6. устойчивость к воздействию окружающей среды;
7. высокая степень безопасности.

Недостатки радиочастотной идентификации:

1. Высокая стоимость системы;
2. Возможность подмены RFID-меток;
3. Сложность самостоятельного изготовления;
4. Подверженность помехам в виде электромагнитных полей;
5. Недостаточная открытость выработанных стандартов.

Сфера применения RFID-технологии постоянно расширяется. Основными областями применения технологии радиочастотной идентификации являются:

1. В библиотеках и архивах:

- антикражные системы;
- оборудование пунктов приема и выдачи книг;
- инвентаризация и поиск книг.

2. Идентификация автомобильного транспорта:

- системы учета автомобилей;
- оборудование пропускных пунктов.

3. В области железнодорожного транспорта:

- системы слежения за локомотивами, пассажирскими и грузовыми вагонами;
- применение в логистике.

4. В добывающей промышленности:

- системы слежения за строительной и специализированной техникой;
- контроль возвратной тары.

5. Идентификация личности:

- применение в системах лояльности розничной торговли;
- применение в системах управления и контроля доступом;
- применение в фитнес-залах и прочих сферах с аналогичными бизнес-процессами.

6. Транспортная логистика:

- повышение эффективности управления поставками;
- мониторинг контейнеров;
- контроль возвратной тары;
- инвентаризация и учет продукции.

Кроме уже существующих способов применения RFID, которые будут совершенствоваться и далее, есть множество областей, готовых принять технологию.

Биометрическая идентификация

Кардинальным решением задачи повышения защиты объекта от несанкционированного доступа является использование биометрической идентификации, которая более эффективна, так как опознание производится не по присвоенным человеку идентификационным признакам, а по физиологическим свойствам или особенностям самого человека – уникальной персональной информации, которую не нужно держать в памяти, невозможно потерять и имитация которой крайне затруднительна [15].

Основное отличие биометрического способа идентификации от других технологий состоит в том, что решения принимаются системой на основе вероятностного характера полученной информации [16]. В этом случае ошибки в принятии решений

неизбежны, и можно говорить только о снижении вероятности появления ошибок. Уровень этих ошибок является основным критерием качества системы.

Этот критерий определяется двумя техническими характеристиками [17]:

1. вероятность несанкционированного допуска (ошибка первого рода) – выраженное в процентах число допусков системой неавторизованных лиц;

2. вероятность ложного задержания (ошибка второго рода) – выраженное в процентах число отказов в допуске системой авторизованных лиц.

Величина ошибки первого рода определяет защищенность системы от несанкционированного допуска, и снижение ее величины более важно, чем ошибки второго рода. Ошибка второго рода в основном влияет на пропускную способность системы.

К распространенным биометрическим методам идентификации относятся:

1. по отпечатку пальца;
2. по форме ладони;
3. по сетчатке глаза4
4. по изображению или форме лица;
5. по ДНК.

Отслеживание скорости и интервалов между нажатиями клавиш при вводе пароля с клавиатуры.

Другие методы (по подногтевому слою кожи, по объему указанных для сканирования пальцев, форме уха, запаху тела и др.).

Достоинства биометрических систем:

1. высокая степень секретности;
2. исключение возможности потери идентификатора или забывания кода;
3. удобство использования (идентификатор всегда с собой);
4. уникальность идентификационных признаков;
5. высокая степень достоверности.

К недостаткам можно отнести:

1. высокая цена;
2. ограничение по числу пользователей;

3. невозможность использования временных пропусков.

Биометрические технологий идентификации представляют собой быстро развивающееся научно-техническое направление, в результатах которого остро нуждаются такие области применения, как системы охраны и контроля доступа, системы паспортного и визового контроля, системы предупреждения преступлений и идентификации преступников, системы учета и сбора статистики посетителей, системы идентификации удаленных пользователей и др.

Кроме того, биометрия может использоваться в спортивных, медицинских, телекоммуникационных, развлекательных и других целях, связанных с выделением и измерением различных биологических характеристик человеческого тела, жестов, движений и т.п.

Идентификация на основе карт с магнитной полосой

Технология магнитных карт получила широкое распространение в кредитно-финансовой области и в системах контроля физического доступа [18].

Для записи двоичного кода используется полоска магнитного материала, нанесенного вдоль края карты. Магнитные полосы изготовлены из материалов, требующих сильных магнитных полей для записи и уничтожения информации, с целью сохранности информации от случайного размагничивания, что в свою очередь затрудняет стирание и видоизменение информации и обеспечивает более высокую степень безопасности.

Классические дебетовые и кредитные карты с магнитной полосой могут использоваться в системах контроля и управления доступом, однако, ввиду некоторых технических особенностей это нежелательно, так как информация на таких картах легко поддается стиранию и перезаписи.

Для использования в системах контроля и управления доступом предназначены специальные карты, называемые высококоэрцитивными, стирание и видоизменение информации на которых затруднено, что обеспечивает более высокую степень безопасности [19].

К достоинствам данной технологии относят:

1. низкая стоимость;
2. возможность перекодирования.

Из недостатков данной технологии выделяют:

1. низкий уровень безопасности;
2. недолговечность;
3. контактная технология считывания;
4. низкая помехозащищенность;
5. плохая устойчивость к механическим повреждениям;
6. низкая пропускная способность.

Заключение

Развитие современного общества тесно связано с ростом информационной составляющей и, как следствие, информационной безопасности. В настоящее время сложно представить ИС, не использующую хотя бы одну из технологий идентификации.

Выбор технологии идентификации зависит от решаемых системой задач. Для учета продукции и товаров подходят штрих-кодовая или радиочастотная технологии, для входа в систему парольная или биометрическая, для систем контроля и управления доступом в помещении подходят радиочастотная или магнитная.

В последнее время, для обеспечения наибольшей безопасности используются комбинированные технологии идентификации [20]. Комбинированные методы позволяют исключить недостатки одной технологии путем использования достоинств другой технологии.

Таким образом, идентификация в ИС, является неотъемлемой частью системы, и именно от реализации процессов идентификации зависит безопасность, точность и скорость работы всей системы.

Литература

1. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие. - СПб.: Изд-во СПбГУЭФ, 2013. - 267 с.

2. Обзор технологий идентификации и аутентификации //URL: https: http://www.infosecurity.ru/ (дата обращения: 01.10.2015)

3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия - Телеком, 2000. – 452 с.

4. Парольная защита: прошлое, настоящее, будущее //URL: http://compress.ru/ (дата обращения: 14.10.2015)

5. Идентификация и аутентификация, управление доступом //URL: https:// http://www.intuit.ru/ (дата обращения: 15.10.2015)

6. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

7. Сабанов А.В. О технологиях идентификации и аутентификации. CONNECT. Мир связи,2006. №3. – С.4-8

8. Арманд В.А., Железнов В.В. Штриховые коды в системах обработки информации Электроннный ресурс]. – Режим доступа: http://www.retail.ru/biblio.

9. Штриховой код //URL: https://ru.wikipedia.org/ (дата обращения: 29.10.2015)

10. Двухмерные штрих-коды //URL: http://www.ibs.ua/spravka/181/ (дата обращения: 29.10.2015)

11. Технология RFID. Опыт использования и перспективные направления. Компоненты и технологии, 2005. – №9. – С.4-8

12. Черепков С. Стандарты и тенденции развития RFID-технологий. Компоненты и технологии, 2006. № 1. – С.8-12

13. Радиочастотная идентификация //URL: http://www.ibs.ua/spravka/181/. (дата обращения: 07.11.2015)

14. Гудин М., Зайцев В. Технология RFID: реалии и перспективы. Компоненты и технологии, 2003. №4. – С.11-13

15. Современные биометрические методы идентификации //URL: http://www.intuit.ru/ (дата обращения: 20.11.2015)

16. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. Пенза: Изд-во Пенз. гос. ун-та, 2000. – 188 с.

17. Барсуков В.С. Интегральная защита информации. Системы безопасности, 2002. №5. – С.8-9

18. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия – Телеком, 2010. – 272 с.

19. Тарасов Ю.А. Контрольно-пропускной режим на предприятии. Защита информации. Конфидент, 2002. – № 1. – С.5-10

20. Ярочкин В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.