А.А. ФОМИН, А.А. ТРИФОНОВ

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

Метод комбинированной идентификации сотрудников предприятия

УДК 004.056.53

В статье проведен обзор комбинированных методов идентификации, рассмотрен комбинированный метод на основе радиочастотной и биометрической идентификации.

Введение

В настоящее время, каждая организация, старается максимальным образом обеспечить защиту предприятия от несанкционированного доступа, такого как проход на территорию, доступ к помещениям, к данным или к секретным документам [1].

Одним из основных методов защиты является идентификация сотрудников [2]. Идентификация может осуществляться в контрольно-пропускном пункте предприятия, перед входом в отдельные кабинеты, доступные не всем сотрудникам организации, при авторизациях в автоматизированных системах и т.д.

Существует множество методов идентификации, которые предназначены для выполнения функции опознавания человека по определенным признакам.

Комбинированные методы идентификации

В последнее время, для обеспечения наибольшей безопасности используются комбинированные технологии идентификации. Комбинированные методы позволяют исключить недостатки одной технологии путем использования достоинств другой технологии [3].

Комбинирует такие методы идентификации как:

- парольная и штрих-кодовая. Чаще всего, данный метод используется в товарообороте и не направлен на увеличение безопасности, а служит подменой одного метода другим [4]. Например, при неудачном считывании штрих-кода, код вводится вручную.

- парольная и биометрическая. Используется при авторизациях пользователей в системах. Увеличивает защиту от несанкционированного доступа путем двухуровневой идентификации, где помимо ввода пароля, необходимо пройти и биометрическую проверку [5].

- радиочастотная и биометрическая. Используется в контрольно-пропускных пунктах и при авторизациях пользователей в системе [6]. Вместо ввода пароля вручную, прикладывается метка с кодом, далее производится биометрическая проверка.

Для идентификации сотрудников, где важна не только защита от несанкционированного доступа, но и пропускная способность идентификации, наибольшее распространение получили комбинированные методы, основанные на радиочастотной и биометрической технологиях [7].

Радиочастотная идентификация

Радиочастотная идентификация производит считывание и запись данных с помощью радиосигналов.

Система идентификации состоит из радиочастотных меток, которые идентифицируют объект, и считывающего устройства, позволяющего считывать данные с меток [8].

Главным достоинством данной технологии является однозначная идентификация при высокой скорости считывания [9]. Существенным недостатком данной технологии, является возможность подмены RFID-метки [10]. Получив чужую метку, злоумышленник получает права доступа сотрудника, которому принадлежит данная метка.

Биометрическая идентификация

Биометрической идентификации основывается на опознавании объекта по физиологическим свойствам или особенностям самого человека. Данное свойство является уникальной персональной

информацией, которую не нужно держать в памяти, невозможно потерять и имитация которой крайне затруднительна [11].

К биометрическим методам могут относится распознавание по отпечатку пальца, по сетчатке глаза, по изображению или форме лица и т.д.

При всех достоинствах данной реализации возникает сложность в скорости идентификации, при регистрации большого объема пользователей в системе, так как для идентификации объекта потребуется проанализировать и сопоставить свойства всех пользователей со свойством идентифицируемого объекта (Рисунок 1).

Рис.1. Схема биометрической идентификации объекта

Комбинированный метод идентификации на основе радиочастной и биометрической технологий

Комбинированный метод позволяет исправить недостатки описанных ранее методов и повысить уровень защиты от несанкционированного доступа [12].

Данная идентификация является двухуровневой. На первом уровне выполняется радиочастотная идентификация, которая определяет какому объекту принадлежит RFID-метка. Если доступ по данной метке разрешен, система идентификации переходит на второй уровень. На втором уровне считываются биометрические данные объекта и сравниваются с биометрическими данными полученного объекта на первом этапе, если данные совпали, то объект успешно прошел идентификацию (Рисунок 2).

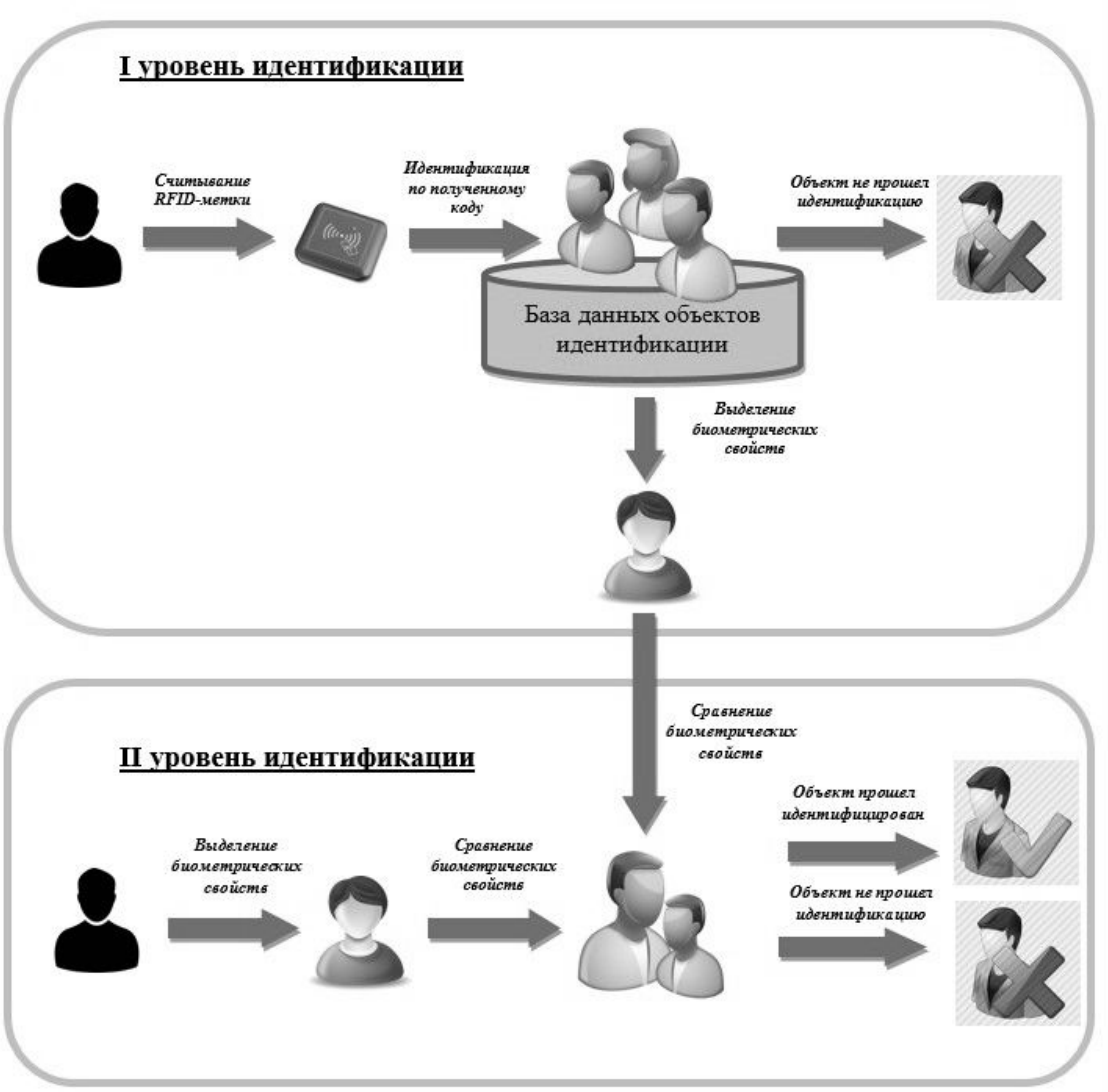

Рис.2. Схема комбинированного метода идентификации на основе радиочастотной и биометрической технологий

При использовании данного комбинированного метода возможность подмены RFID-метки исключается, так как злоумышленник не сможет пройти второй уровень идентификации, в то же время скорость работы биометрической идентификации увеличится, так как объект идентификации будет сопоставляться не со всеми объект системы, а только с тем, который был идентифицирован при радиочастотном считывании [13].

Для организации данного комбинированного метода идентификации необходимо следующее оборудование:

1. радиочастотный считыватель – для радиочастотной идентификации;

2. биометрический считыватель – устройство зависит от выбранного метода биометрической идентификации:

- Веб-камера;
- Сканер отпечатков пальцев;
- Сканер сетчатки глаза;
- Микрофон.

3. ПК – выполняет вычислительные операции по идентификации объектов, а также служит узлом связи с базой данных и устройствами считывания.

Пример структуры системы идентификации на основе комбинированного метода радиочастной и биометрической технологий представлен на рисунке 3.

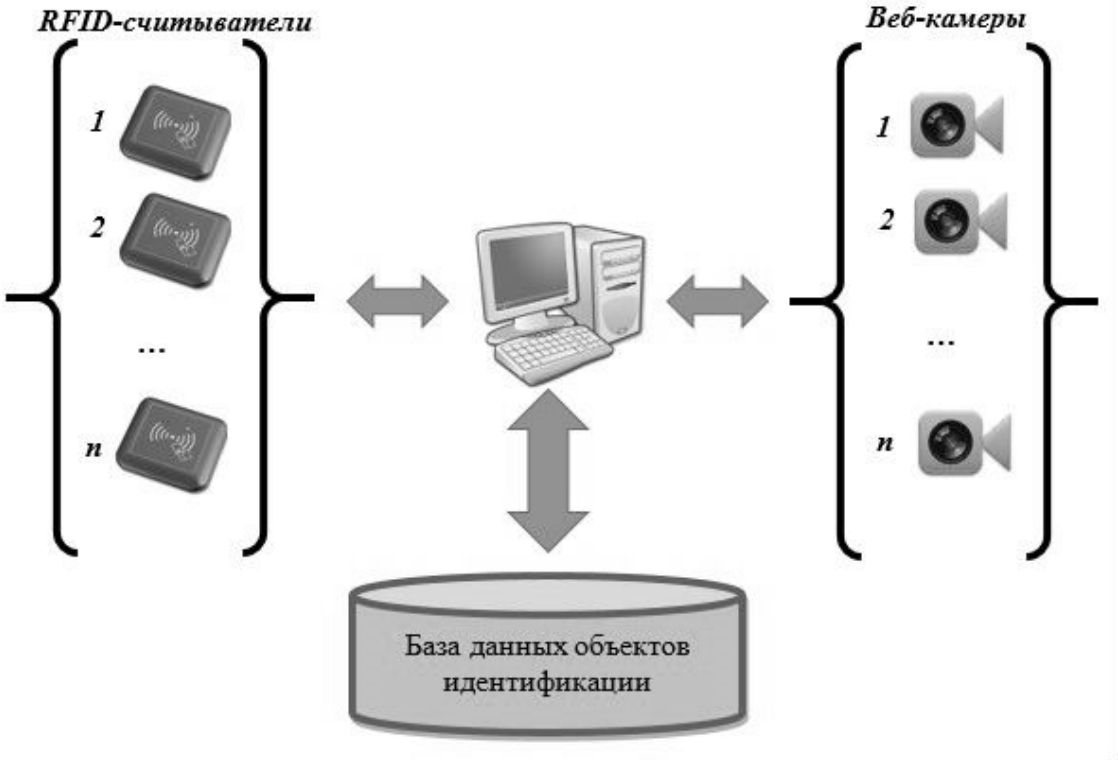

Рис.3. Структура системы комбинированного метода идентификации на основе радиочастной и биометрической технологий

Заключение

Рост информационной составляющей тесно связано с ростом информационной безопасности. Одним из наиболее перспективных направлений защиты от несанкционированного доступа на предприятии, является идентификация сотрудников [14].

Главными параметрами в идентификации является надежность и скорость [15]. При увеличении надежности, скорость идентификации может значительно упасть, что в некоторых случаях может привезти к негативным последствиям. И наоборот при увеличении скорости, путем уменьшения уровней защиты, главным образом страдает надежность идентификации. Поэтому, при выборе технологии, необходимо взвесить такие значения, как важность данных и скорость доступа к ним, и уже в зависимости от этого, выбирать наиболее подходящий метод.

Литература

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

2. 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.

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

4. Арманд В.А., Железнов В.В. Штриховые коды в системах обработки информации //URL: http://www.retail.ru/biblio. (дата обращения: 11.10.2016)

5. Парольная защита: прошлое, настоящее, будущее //URL: http://compress.ru/ (дата обращения: 20.10.2016)

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

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

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

9. Радиочастотная идентификация //URL: http://www.ibs.ua/spravka/181/. (дата обращения: 28.10.2016)

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

11. Современные биометрические методы идентификации //URL: http://www.intuit.ru/ (дата обращения: 08.11.2016)

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

13. Обзор технологий идентификации и аутентификации //URL: https: http://www.infosecurity.ru/ (дата обращения: 10.11.2016)

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

15. Идентификация и аутентификация, управление доступом //URL: https:// http://www.intuit.ru/ (дата обращения: 12.11.2016)