

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/diplomnaya-rabota/206530>

Тип работы: Дипломная работа

Предмет: Информатика основы

Введение 2

1. Обзор применяемых методик оценки надежности биометрических систем аутентификации 4

1.1 Основные направления и объекты использования биометрических систем 4

1.2. Анализ методов обработки результатов ошибок 1 и 2 рода при распознавании объектов с помощью биометрических данных 8

1.3. Статистические методы, применяемые для идентификации, верификации, аутентификации, распознавания в системах 11

2. Описание биометрической системы и моделирование угроз безопасности биометрической системы банка 16

2.1. Объект защиты и его свойства 16

2.2. Построение модели угроз безопасности биометрической системы банка 18

2.3. Анализ актуальных угроз безопасности биометрической системы банка 20

3. Построение системы защиты биометрической системы банка 27

3.1. Анализ средств и методов защиты биометрической системы 27

3.2. Выбор программных систем управления видеонаблюдением 39

3.3. Оценка надежности системы безопасности биометрической системы 49

ЗАКЛЮЧЕНИЕ 54

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 57

Приложение 1 61

Введение

В настоящее время одним из методов авторизации в информационных системах является парольная защита. Данный способ авторизации в системе не обеспечивает полноценной защиты от несанкционированного доступа, так как сотрудники зачастую не соблюдают требований к защите паролей, передавая их коллегам или оставляя парольные карточки на доступных местах. Также вероятно использование паролей, не отвечающих требованиям к сложности, отчего возрастает вероятность получения доступа к информационным ресурсам со стороны злоумышленников. Когда ценность информационного ресурса достаточно высока (например, при работе с серверами, межсетевыми экранами, платежными системами) требуется использование усиленных мер защиты при входе в систему. К ним относятся: электронные ключи, а также биометрические системы. При использовании электронных ключей также существует риск утери и передачи. Таким образом, наиболее надежным методом аутентификации являются способы, связанные с биометрическими технологиями, позволяющими однозначно определить личность пользователя, осуществляющего попытку входа в систему.

Целью дипломной работы – изучение безопасности внутрибанковской биометрической системы и разработка комплекса мер по ее обеспечению.

Задачи исследования:

анализ технологий защиты систем биометрической аутентификации;

выбор методов, обеспечивающих технологии защиты систем биометрической аутентификации;

разработка системы информационно-аналитической поддержки контрольно-пропускной системы с использованием биометрических параметров.

Объект исследования: системы биометрической аутентификации в охранных системах.

Предмет исследования: технология биометрической идентификации в условиях банковского учреждения.

Методы исследования: анализ литературных источников, синтез, моделирование, обобщение, наблюдение.

Гипотеза исследования: внедрение системы защиты (или защищенной) межбанковской биометрической системы позволит повысить уровень физической защиты предприятия, сократить убытки, обусловленные возникновением инцидентов, связанных с информационной безопасностью

1.1 Основные направления и объекты использования биометрических систем

Биометрические системы аутентификации — системы, использующие для входа в систему биометрические методы. С помощью биометрических систем авторизации определяется подлинность пользователя, совершающего попытку авторизации в системе.

Проблематика использования биометрической идентификации в различных технических системах в настоящее время является объектом изучения авторов, работающих в различных научно-технических областях. В работе Аюповой А. Р., Ахатов Р. Р. «Биометрический паспорт: зло или добро» рассмотрены вопросы создания биометрических паспортов граждан, что упрощает их процессы их идентификации. Вместе с этим утечки биометрических данных могут привести к различным негативным последствиям для объекта. В работе Михайлова М. А., Волеводза А. Г., Сидоренко Э. Л. «Совершенствование системы дактилоскопической регистрации» рассмотрены правовые и технологические аспекты перспективного использования биометрических данных при аутентификации в банковских системах, портале госуслуг. Данная технология позволит обеспечить достоверность определения пользователя системы, но вместе с этим связана с необходимостью приобретения считывателей и гарантированного обеспечения защиты биометрических данных.

Использование современных биометрических систем позволяет обеспечить высокий уровень надежности при аутентификации объектов. Контроль с помощью биометрии возможно обеспечить в следующих областях [12]:

- при передаче и получении конфиденциальных данных;
- при авторизации в информационных системах;
- при проведении платежных операций;
- для обеспечения защиты баз данных и любых конфиденциальных данных на электронных носителях;
- при работе с системами контроля управления доступом;
- для доступа к системам «умного дома» для управления системами жизнеобеспечения помещений.

Специфика использования биометрических систем связана с возможностью однозначного распознавания объекта без возможности подделки.

К биометрическим факторам относятся [11]:

- отпечатки пальцев;
- рисунок радужной оболочки и сетчатки глаз;
- характеристики голоса;
- геометрический рисунок руки;
- ДНК.

Эффективность работы биометрических идентификаторов обеспечивается в тех случаях, когда имеется достоверная возможность установки факта принадлежности биометрического отпечатка конкретному субъекту и при проверке факта полного совпадения биометрического отпечатка эталону, хранящемуся в картотеке.

В силу того, что биометрическая аутентификация находит все более широкое использование, у операторов, проводящих обработку данного рода информации, должны обеспечиваться требования к сохранности информации.

Основные характеристики систем биометрической аутентификации [10]:

- диапазон вероятности несанкционированного доступа - 0,1–0,0001 %;
- вероятность ложного запрета доступа субъекта к своим данным 1%;
- время идентификации субъекта - 10 сек.

При этом для систем биометрической аутентификации характерна высокая стоимость в сравнении с традиционными методами (по паролю или по электронному ключу)

К динамическим методам биометрии можно отнести: исследование почерка, особенности голоса и речи. На рисунке 1 приведена диаграмма классификации биометрических средств идентификации.

Рисунок 1 - Диаграмма классификации биометрических средств идентификации [3]

Тенденции к совершенствованию характеристик систем биометрической идентификации и снижению их стоимости постепенно приводят к расширению областей применения систем биометрической

идентификации [21]. На рисунке 2 приведена диаграмма распространенности систем биометрической идентификации.

Рисунок 2 – Распределение технологий распознавания объектов с использованием систем биометрии [2]

Распознавание объектов с использованием технологий биометрии включает стадии [7]:

получение данных биометрических образов;
определение шаблона для проведения сверки;
сравнение считанного образца с эталонным.

Далее система при идентификации объекта предоставляет возможности доступа в соответствии с назначенной ролью. Если объект не распознан, доступ не предоставляется.

Обобщая, заметим, что в настоящее время широкое развитие приобретают системы биометрической аутентификации, достоинством которых является возможность однозначного распознавания объекта. Алгоритмы распознавания основаны на сравнении объекта с шаблонами. В качестве идентификаторов могут выступать отпечатки пальцев, оболочка глаз и другие объекты, позволяющие однозначно идентифицировать объект.

1.2. Анализ методов обработки результатов ошибок 1 и 2 рода при распознавании объектов с помощью биометрических данных

При использовании систем биометрии возможно возникновение коллизий, связанных с ошибками распознавания, включающих [3]:

ошибки первого рода, при возникновении которых блокируется доступ пользователям, которые внесены в базу и имеют право входа в систему;

ошибки второго рода, при возникновении которых система сопоставляет определенную роль для пользователей, которые доступа к системе не имеют.

Возникновение ошибок подобного типа связано со спецификой биометрии, к которых точность распознавания зависит от разрешающей способности биометрических сканеров, качества работы программного обеспечения, осуществляющего сопоставление объекта с эталоном. Например, в случае сканирования отпечатков пальцев невозможно установить полное соответствие эталонному положению, так как может отличаться угол сканирования, давление пальца на считыватель и другие параметры, оказывающие влияние на результат процесса идентификации.

Таким образом, биометрические процессы (связанные с автоматизированной обработкой характеристик) обеспечивают уровень надежности, обеспечиваемой биометрической системой при распознавании объекта. Система не может давать заключение о полном соответствии снимка с копией, а выдает вероятность того, что отпечаток биометрического объекта соответствует определенному эталону в базе данных. При приближении данного значения к 100% достоверности установления личности повышается. В ходе опыта работы с биометрическими было показано, что хотя ни одной системой аутентификации не обеспечивается 100 %-ный уровень надежности и совпадения характеристик, уровень совпадения является достаточно высоким.

Существующие системы биометрической идентификации позволяют обеспечивать высокий уровень устойчивости к ошибкам первого и второго рода при определении объекта.

Так как степень надежности в процессе проведения операций сравнения зависит от специфики объекта авторизации, чрезвычайным является оценка влияния ложного срабатывания на возможность доступа к системе посторонних лиц. Разработчиками гарантируется уровень точности измерений, соответствующий одной ошибке на 10 000 измерений.

Качество распознавания в система биометрии характеризуется показателями [4]:

FAR (False Acceptance Rate) – параметр, характеризующий количество допусков в систему объектам, не зарегистрированным в базе данных эталонных объектов.

FRR (False Rejection Rate) – параметр, характеризующий количество запретов на вход в систему пользователям, имеющим к ней доступ.

Для каждой биометрической системы опытным путем проводится расчет данных качественных характеристик, по результатам которого делается заключение о возможности ее использования применительно к защищаемому объекту.

Статистические данные показывают информацию по качеству работы объектов в зависимости от

распознаваемой биометрической системы (таблица 1).

Таблица 1 – Качественные характеристики биометрических объектов

При использовании биометрических систем также возможна работа с более точными показателями, при этом такие биометрические системы при распознавании используют более сложные алгоритмы, требующие значительных вычислительных мощностей.

Возможно получение статистических доказательств, позволяющих с помощью компьютерных программ провести соответствующие расчеты, посредством которых подтверждаются указанные цифры, однако на практике ложные срабатывания могут случаться гораздо чаще [19].

Надежность процедуры идентификации по отпечаткам обеспечивается при гарантированной защите от копирования эталонной базы данных. В качестве одной из возможностей по обману терминалов специалистами называется способ изготовления искусственной кисти с необходимыми отпечатками пальцев (или через изъятие «подлинника» у законных владельцев). Также существует метод борьбы с таким типом фальсификации. Для защиты от несанкционированной идентификации в считыватели оборудования включают инфракрасные детекторы, позволяющий фиксировать исходящее инфракрасное излучение от объекта и при его отсутствии доступ блокируется.

Защита от авторизации с использованием копий папиллярных узоров обеспечивается путем получения от объекта дополнительной информации, которой злоумышленники не обладают.

Это порождает ряд проблем, связанных с быстродействием систем распознавания, а также необходимостью защиты от подлога. При корректно настроенных алгоритмах распознавания и использовании сертифицированного программного обеспечения возможно обеспечение безошибочного распознавания объектов.

1.3. Статистические методы, применяемые для идентификации, верификации, аутентификации, распознавания в системах

Математическая модель анализа биометрических данных основана на усреднении функции по частотным диапазонам, весовые коэффициенты которой описывается через функцию и выражения:

С использованием функции $f(x,y)$ можно решить задачу по идентификации обрабатываемого изображения через две пространственные переменные, заданные в определенной области пространства прямоугольной формы.

Проведем анализ работы с двумерными системами, содержащими линейные функции [30].

В рамках моделирования биометрических объектов осуществляется преобразование функции вида:

$$g(x,y)=L(f(x,y))$$

Моделируемую систему можно рассматривать через пространственно-инвариантные характеристик, если значения ее импульсных откликов определяется через разность координат входных и выходных (x, n) плоскостей. В оптических системах, пример которых показан на рисунке 3, предполагается, что в случае перемещения точечного источника в наблюдаемой плоскости может изменять положение, но при этом форма сохраняется [16].

1. ПО Bio Time. Описание. [Электронный ресурс]. Режим доступа:

<https://www.bioblink.ru/products/software/biotime/overview.php>

2. Аюпова А. Р., Ахатов Р. Р. Биометрический паспорт: зло или добро // Здоровый образ жизни как условие устойчивого развития государства: сборник материалов Всероссийской научно-практической конференции. — 2017. — С. 35—38.

3. Кубитович С. Н. ДНК как носитель информации неограниченного круга лиц // Вестник экономической безопасности. — 2017. — № 4. — С. 184—188.

4. Михайлов М. А., Волеводз А. Г., Сидоренко Э. Л. Международная научно-практическая конференция в Государственной Думе «Совершенствование системы дактилоскопической регистрации» // Библиотека криминалиста. Научный журнал. — 2016. — № 1 (24). — С. 368—378.

5. Попов В. В. Идентификация личности молекулярно-генетическими методами // Юристъ-Правоведъ. 2018. № 3 (86). С. 169—175.

6. Милов, В. Р. Распознавание образов и обработка изображений в информационно-аналитических системах:

- мониторинг, проектирование / В. Р. Милов, В. Г. Баранов, Ю. С. Бажанов и др. - Москва : Радиотехника, 2014. - 143 с.
7. Кретушев А. В. Обработка и анализ фазовых изображений: учебное пособие / А. В. Кретушев. - Москва : ВНИИгеосистем, 2014. - 63 с.
8. Шоберг А. Г. Современные методы обработки изображений: модифицированное вейвлет-преобразование / А. Г. Шоберг. - Хабаровск: Изд-во ТОГУ, 2014. - 125 с.
9. Гришенцев, А. Ю. Методы и модели цифровой обработки изображений / А. Ю. Гришенцев, А. Г. Коробейников. - Санкт-Петербург: Изд-во Политехнического ун-та, 2014. - 189 с.
10. Можаров, Г. П. Основы цифровой вейвлет-обработки сигналов и изображений / Г. П. Можаров. - Москва: МГТУ, 2014
11. Панин, С. Д. Теория принятия решений и распознавание образов: курс лекций /С.Д. Панин. - Москва: Изд-во МГТУ, 2017. - 239 с.
12. Васильев, К. К. Статистический анализ последовательностей изображений: [монография] / К.К. Васильев, В.Р. Крашенинников. - Москва : Радиотехника, 2017. - 246 с.
13. Бахрушина Г. И. Цифровое маркирование изображений: монография / Г. И. Бахрушина, А. П. Бахрушин, А. Н. Иванов. - Хабаровск: Изд-во ТОГУ, 2017. - 325с.
14. Умняшкин С. В. Основы цифровой обработки изображений : учебное пособие / С. В. Умняшкин, В. В. Лесин. - Москва: МИЭТ, 2016. - 200 с.
15. Кувшинов Б. М. Нейронные сети: учебное пособие: / Б. М. Кувшинов. - Челябинск : Издательский центр ЮУрГУ, 2015. - 65 с.
16. Курзаева Л. В. Нечеткая логика и нейронные сети [Электронный ресурс]: учебное наглядное пособие / Л.В. Курзаева. - Магнитогорск : ФГБОУ ВПО "МГТУ", 2015.
17. Хливненко Л. В. Практика нейросетевого моделирования / Л. В. Хливненко. - Воронеж: Воронежский государственный технический университет, 2015. - 214 с.
18. Кузнецова О. Ю. Основы нечетких множеств и нечетких нейронных сетей: учебное пособие / О. Ю. Кузнецова, В. И. Горбаченко. - Пенза : Изд-во ПГУ, 2015. - 97 с.
19. Васильков, А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. - М.: Форум, 2013. - 528 с.
20. Кузнецов В.В. Защищенная биометрическая идентификация по изображению отпечатка пальца/ Кузнецов Владислав Владимирович. - Москва.: Инфра-М, 2013. - 26 с.
21. Польшакова Н.В., Коломейченко А.С., Яковлев А.С. Информационные системы в экономике: [учебник]. - Москва: Буки Веди, 2016. - 480 с.
22. Венделева, М.А. Управленческие информационные системы/ М.А. Венделева, Ю.В. Вертакова. - М.: Юрайт, 2013. - 462 с.
23. Герчикова Т.М.: Разработка информационных систем. - М.: Бук-Пресс и К, 2015
24. Исакова А.И. Основы информационных технологий [Электронный ресурс]: учебное пособие / А.И. Исакова. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. - 206 с
25. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с.
26. Шеховцов О. И. Корпоративные информационные системы: учебное пособие / О. И. Шеховцов. - Санкт-Петербург : СПбГУТ, 2016. - 59 с.
27. Козак М. Ф., Козак М. В. Биометрические методы в научных исследованиях: монография / М.Ф. Козак, М.В. Козак. - Астрахань: Астраханский университет, 2019. - 167 с.
28. Стружкин, Н. П. Базы данных: проектирование. Практикум: учебное пособие / Н. П. Стружкин, В. В. Годин. — Москва: Издательство Юрайт, 2022. — 291 с.
29. Алюшин М.В., Алюшин В. М. Цифровые биометрические технологии: учебное пособие / М.В. Алюшин, В.М. Алюшин. - Москва : Национальный исследовательский ядерный университет "МИФИ", 2018. - 215с.
30. Полякова, Т.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов . — Москва: Издательство Юрайт, 2022. — 325 с.
31. Авдеев В. И. Современные методы биометрии в исследовании растений : учебное пособие / В. И. Авдеев. - Оренбург: ОГАУ, 2015. - 127 с.
32. Юрченко Е. Н., Иванова И. П. Биометрия: учебное пособие / Е. Н. Юрченко, И. П. Иванова. - Омск: Изд-во ФГБОУ ВО Омский ГАУ, 2015. - 87 с.

33. Артемьева Е. А., Чарыкова А. Ф. Биометрия с основами математических методов в биологии: учебник / Е. А. Артемьева, А. Ф. Чарыкова. - Ульяновск: Корпорация технологий продвижения, 2017. - 135 с.
34. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2022. — 309 с.
35. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — Москва: Издательство Юрайт, 2022. — 161 с.
36. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с.
37. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2022. — 349 с.
38. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с.
39. Нетёсова, О. Ю. Информационные системы и технологии в экономике: учебное пособие для вузов / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — Москва: Издательство Юрайт, 2022. — 178 с.
40. Стасышин, В. М. Базы данных: технологии доступа: учебное пособие / В. М. Стасышин, Т. Л. Стасышина. — Москва : Издательство Юрайт, 2022. — 164 с.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/diplomnaya-rabota/206530>