УДК 004.056

АНАЛИЗ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕОБХОДИМЫХ ПРИ ПРОХОЖДЕНИИ ПРОПУСКНОГО БИОМЕТРИЧЕСКОГО КОНТРОЛЯ НА ПРЕДПРИЯТИИ

Неделько Я. В.[1]

ст. препод. **Мозговенко А.А.**[1]

[1]*Федеральное государственное бюджетное образовательное учреждение высшего образования (ФГБОУ ВО) «Мелитопольский государственный университет», г.Мелитополь ya@amozgovenko.ru*

Аннотация: *В статье проводится анализ мер информационной безопасности, необходимых при прохождении биометрического контроля на предприятии. Рассматриваются различные технологии идентификации личности, такие как распознавание лиц, сканирование отпечатков пальцев и радужной оболочки глаза. Обсуждаются преимущества и недостатки каждой технологии, а также возможные угрозы и риски, связанные с их использованием. Особое внимание уделяется вопросам защиты персональных данных и конфиденциальности информации сотрудников предприятия.*

Ключевые слова: *биометрика, распознание лиц, обработка изображений, собственные векторы.*

ANALYSIS OF INFORMATION SECURITY MEASURES REQUIRED WHEN PASSING BIOMETRIC ACCESS CONTROL AT AN ENTERPRISE

Nedelko Y. V..1

Senior Lecturer Mozgovenko A.A.1

[1]*Federal State Budgetary Educational Institution Higher Education (FSBEI HE) "Melitopol State University", Melitopol*

Abstract: *The article analyzes the information security measures required for biometric control at an enterprise. Various technologies for identifying individuals, such as facial recognition, fingerprint and iris scanning, are considered. The advantages and disadvantages of each technology, as well as possible threats and risks associated with their use, are discussed. Particular attention is paid to the protection of personal data and the confidentiality of information of enterprise employees.*

Keywords: *biometrics, face recognition, image processing, eigenvectors.*

Введение.

В современном мире информационная безопасность становится всё более актуальной проблемой, особенно на предприятиях, где хранятся и обрабатываются большие объёмы данных. Одним из эффективных способов обеспечения безопасности является использование биометрических технологий, в частности, биометрического контроля доступа. В этой статье мы проведём анализ мер информационной безопасности, необходимых при прохождении такого контроля на предприятии.

Актуальность темы связана с ростом числа кибератак и утечек данных, что приводит к серьёзным финансовым потерям и репутационным рискам для компаний. Биометрический контроль доступа обеспечивает более высокий уровень безопасности, так как он основан на уникальных физиологических и поведенческих характеристиках человека, что затрудняет подделку идентификационных данных.

Научная новизна статьи заключается в комплексном анализе существующих методов и подходов к обеспечению информационной безопасности при использовании биометрических систем контроля доступа на предприятии. В работе рассматриваются основные угрозы и риски, связанные с применением биометрических технологий, а также предлагаются новые подходы к повышению уровня безопасности и снижению вероятности несанкционированного доступа к информационным ресурсам компании.

Цель исследования — проанализировать российские и международные практики в области информационной безопасности при использовании биометрических систем контроля доступа на предприятии.

Материал и методы исследования

В ходе исследования, были проанализированы научные работы отечественных и зарубежных ученых, был проведен анализ существующего программного обеспечения для распознавания лиц и разработан программный продукт.

Результаты исследования и их обсуждение

Пропускной контроль на предприятии — это система, обеспечивающая безопасность работников, материальных ценностей и информационных ресурсов. Он включает в себя контроль доступа сотрудников, посетителей и автотранспорта на территорию предприятия. Пропускной режим может быть обязательным (например, в школах, вузах, предприятиях оборонно-промышленного комплекса) или вводиться по решению работодателя.

Для организации пропускного контроля используются различные физические средства заграждения (турникеты, калитки, шлагбаумы) и технические средства (средства связи, тревожной сигнализации, основное и резервное освещение, видеоконтроль). Пропуска могут быть разовыми,

временными или постоянными, а также бумажными или электронными (пластиковые карты, биометрические данные).

В данной статье мы рассмотрим более подробно пропускной контроль с использованием биометрических данных. Биометрия — это сведения о физиологических и биологических характеристиках человека, с помощью которых можно определить его личность. К наиболее распространённым видам биометрии относятся: отпечаток пальца, изображение лица, голос, радужная оболочка глаза и рисунок вен ладони.

Пропускной контроль с распознаванием лиц — это система, которая использует технологию распознавания лиц для идентификации личности человека. Эта система применяется в системах контроля и управления доступом (СКУД) и системах учёта рабочего времени.

Преимущества такого контроля:

- высокая точность идентификации;
- отсутствие физического контакта и активных действий со стороны пользователя;
- простота процесса регистрации новых сотрудников и загрузки их фотографий.

Однако есть и недостатки:

- проблемы с точностью определения лиц, особенно при групповом проходе;
- необходимость использования дополнительного оборудования (IP-камеры) и программного обеспечения.

Алгоритм прохождения пропускного контроля с распознаванием лиц включает следующие этапы:

1. Захват видеоизображения лица сотрудника на IP-камере, подключённой к СКУД.
2. Сравнение полученного изображения с базой данных лиц сотрудников на основе обычных фотографий.
3. В зависимости от настроек системы возможны два режима идентификации: верификация и идентификация.

В режиме верификации основным идентификатором служит бесконтактная карта, а лицо сотрудника используется как дополнительный признак. Если лицо распознано, система разрешает доступ. В противном случае доступ блокируется.

В режиме идентификации лицо сотрудника является единственным признаком для принятия решения о доступе.

Требования к пропускному контролю с распознаванием лиц включают:

1. Фронтальное расположение лица относительно камеры.
2. Высокое качество изображений и видеозаписи.
3. Равномерное распределение света в зоне работы камеры.
4. Достаточное количество пикселей для корректного отображения лица.

5. Наличие вычислительных ресурсов для обработки изображений и сопоставления их с базой данных.

6. Соблюдение правил безопасности и конфиденциальности данных.

Пропускной контроль с использованием отпечатков пальцев основан на технологии биометрической идентификации. Этот метод использует уникальные узоры на кончиках пальцев для идентификации личности. Процесс регистрации отпечатков прост и быстр, а сама система обеспечивает высокую степень безопасности и надёжности.

Плюсы:

- Высокий уровень безопасности: отпечатки пальцев уникальны для каждого человека, их сложно подделать.
- Удобство использования: быстрый и надёжный способ идентификации.
- Бесконтактный доступ: не нужно прикасаться к датчику, что снижает риск передачи инфекций.
- Высокая точность: современные сканеры обеспечивают высокую точность распознавания отпечатков.

Минусы:

- Возможность загрязнения или повреждения отпечатков пальцев, что может привести к сбоям в работе системы.
- Необходимость регулярного обновления базы данных отпечатков для поддержания точности системы.
- Возможное влияние внешних факторов, таких как влажность или температура, на работу сканера.

Алгоритм прохождения пропускного контроля с отпечатками пальцев состоит из следующих этапов:

1. Регистрация: пользователи регистрируются в системе, предоставляя свои биометрические данные, такие как отпечатки пальцев.
2. Сканирование отпечатков пальцев: при прохождении через пропускной пункт пользователь прикладывает палец к сканеру, который считывает уникальный рисунок отпечатка.
3. Идентификация и сравнение: система сравнивает полученные данные с сохранёнными в базе данных. Если отпечаток совпадает с одним из образцов, пользователю предоставляется доступ.
4. В случае ошибки или несоответствия система может запросить дополнительную проверку, например, ввод пароля или использование другого метода идентификации.

Требования к пропускному режиму с использованием отпечатков пальцев могут быть следующими:

1. Согласие работников на проведение дактилоскопии.
2. Письменное заявление гражданина для добровольной государственной дактилоскопической регистрации (статья 8 Закона № 128-ФЗ).

3. Обработка и использование отпечатков пальцев только с письменного согласия работников (ч. 4 ст. 9 Закона № 152-ФЗ).

Пропускной контроль по голосу — это метод биометрической идентификации, который использует уникальные характеристики голоса человека для проверки его личности. Этот метод применяется для контроля доступа к информации или помещениям, где требуется дополнительная защита.

Плюсы пропускного контроля по голосу:

- высокая степень надёжности;
- удобство использования;
- бесконтактный доступ;
- возможность интеграции с другими системами безопасности.

Минусы пропускного контроля по голосу:

- зависимость точности идентификации от внешних факторов (температура, влажность, состояние здоровья);
- возможность обмана с помощью специальных устройств или изменения голоса;
- необходимость обучения персонала для правильной настройки и эксплуатации системы.

Алгоритм прохождения пропускного контроля по голосу включает следующие этапы:

1. Регистрация в системе: пользователи регистрируются, предоставляя свои биометрические данные, включая голос.
2. Сканирование голоса: при прохождении через пропускной пункт пользователь произносит фразу, которую система записывает и анализирует.
3. Идентификация и сравнение: система сравнивает полученные данные с сохранёнными в базе данных. Если голос совпадает с одним из образцов, пользователю предоставляется доступ.
4. В случае ошибки или несоответствия система может запросить дополнительную проверку, например, ввод пароля или использование другого метода идентификации.

Требования к пропускному контролю по голосу могут включать:

1. Наличие специализированного оборудования для распознавания голоса, например, аудиоанализаторов или голосовых сканеров.
2. Соблюдение стандартов качества и точности идентификации, установленных производителем оборудования.
3. Регулярное обновление и настройка программного обеспечения для обеспечения корректной работы системы.
4. Обучение персонала правилам работы с оборудованием и процедурами контроля доступа на основе голоса.

Пропускной контроль по радужной оболочке глаза — это метод биометрической идентификации, использующий уникальные характеристики радужки глаза для распознавания личности. Технология

основана на анализе колец, волокон и пигментации радужки, что делает её практически неизменной и уникальной у каждого человека.

Преимущества такого контроля включают высокую надёжность, точность и безопасность, так как подделать радужную оболочку невозможно.

Преимущества:

- Высокая надёжность и точность идентификации благодаря уникальным характеристикам радужной оболочки глаза.
- Безопасность, так как радужную оболочку сложно подделать.
- Возможность бесконтактного доступа без необходимости совершать телодвижения.
- Высокая скорость работы, позволяющая избежать очередей на входе.

Недостатки:

- Более высокая стоимость оборудования и установки по сравнению с другими методами идентификации, такими как отпечаток пальца или Face ID.
- Ограниченная доступность в некоторых странах или регионах из-за недостаточного распространения технологии.

Алгоритм прохождения пропускного контроля по радужной оболочке глаза включает следующие этапы:

1. Получение изображения радужной оболочки с помощью монохромной камеры с инфракрасной подсветкой.
2. Сегментация и параметризация изображения, разделение на сегменты и определение границ радужной оболочки, зрачка и склеры.
3. Извлечение параметров изображения радужной оболочки и сравнение их с базой данных.
4. Идентификация и аутентификация радужной оболочки с использованием алгоритмов сравнения и принятия решения о допуске.
5. Вероятность совпадения двух радужных оболочек составляет 10^(-72), что обеспечивает высокую степень безопасности.

Требования к пропускному контролю по радужной оболочке глаза включают:

- использование специализированных камер для фиксации изображения радужки глаза;
- обработку изображения для выявления уникальных характеристик радужки, таких как кольца, волокна и пигментация;
- преобразование полученных данных в цифровой код, который служит биометрическим ключом;
- сравнение цифрового кода с ключами в базе данных для идентификации личности или верификации.

Пропускная способность системы может достигать 20 человек в минуту, возможна регистрация по одному или двум глазам, а также сочетание идентификации по радужке глаза с другими видами

идентификации, например, по карте.

Пропускной контроль по рисунку вен ладони основан на технологии получения изображения ладони в инфракрасном свете определённой длины волны. В результате сканирования в ИК области спектра становятся видимыми скрытые под кожным покровом вены, образуя уникальный рисунок для каждого человека. Этот рисунок используется для идентификации и доступа к личным данным.

Преимущества:

- Уникальность рисунка вен ладони, что повышает точность распознавания.
- Не зависит от влажности или загрязнения ладони, в отличие от отпечатков пальцев.
- Успешно работает в любое время года и при разных погодных условиях.
- Считается наиболее гигиеничным методом считывания биометрических данных.
- Естественная защита данных, так как рисунок вен ладони невозможно получить с помощью фотоаппарата.

Недостатки:

- Сканер устройства нельзя размещать на улице из-за вероятности засветки солнечными лучами.
- Некоторые заболевания могут изменить рисунок вен, ухудшая точность распознавания.
- Стоимость системы выше, чем у других биометрических методов

Алгоритм прохождения пропускного контроля по рисунку вен ладони состоит из следующих этапов:

1. Получение биометрического образа: пользователь подносит палец или ладонь к специальному сканеру, который делает фотосъёмку в ближнем инфракрасном диапазоне.
2. Фильтрация исходного графического изображения и выделение области интереса.
3. Бинаризация: приведение всех изображений к одному виду.
4. Выделение области интереса: определение «перепонок» между пальцами.
5. Разбиение обработанного изображения на участки дискретизации с указанием координат контрольных точек и углов поворотов линий.
6. Создание математической модели: запись полученных данных в файл.
7. Идентификация происходит путём сравнения полученного шаблона с шаблонами, хранящимися в базе данных.

Требования к пропускному контролю по рисунку вен ладони включают:

1. Бесконтактное сканирование вен ладони на расстоянии до 10 см с помощью сканера PALMJET.

2. Наличие дистанционных термодатчиков для контроля температуры сотрудников на проходной.

3. Использование биометрических терминалов BioSmart Quasar для идентификации сотрудников по лицу и бесконтактных сканеров RFID-карт SMARTKEY на выходах.

4. Полностью автоматизированная проходная с настройкой и интеграцией оборудования для формирования отчётов и удобной работы с системой.

Для обеспечения информационной безопасности при прохождении биометрического пропускного контроля на предприятии необходимо:

1. Использовать надёжные и проверенные технологии биометрической идентификации, такие как распознавание лиц, радужной оболочки глаза или отпечатков пальцев.

2. Обеспечивать конфиденциальность и защиту персональных данных пользователей, соблюдая требования законодательства о защите информации.

3. Внедрять многоуровневую систему аутентификации и авторизации пользователей, включая использование паролей, двухфакторной аутентификации и других методов защиты.

4. Регулярно обновлять программное обеспечение и аппаратные средства системы биометрического контроля, чтобы устранять уязвимости и повышать уровень безопасности.

5. Обучать персонал правилам информационной безопасности, проводить тренинги и семинары по защите персональных данных и использованию систем биометрического контроля.

6. Обеспечивать физическую безопасность оборудования и инфраструктуры системы биометрического контроля, устанавливать системы видеонаблюдения, контроля доступа и пожарной сигнализации.

Список литературы

1. Самаль Д.И. Построение систем идентификации личности на базе антропометрических точек лица // Цифровая обработка изображений. – Минск: Ин-т техн. кибернетики НАН Беларуси, 1998. – С.72-79.

2. Арутненов В. В. Сравнительный анализ биометрических систем защиты информации. - (Организация информационной работы). 2010, №4.

3. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека. - СПб.: Политехника, 2001. - 240 с.

4. Вихман В. В., Биометрические системы контроля и управления доступом в задачах информации: учебно-методическое пособие. — 2016. — 236 стр. Частикова В. А., Васильев Е. Д., Бабич Д. В., Нейросетевая методика идентификации лиц в видеопотоке в условиях ограниченности данных // Вестник АГУ. — 2019. — Т. 3, № 246. — С. 85–89.