МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01ммзи
Ватажок Д.И.
(подпись)

Отчет защищен с оценкой

С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный №
« 31 » июля 2021 г.

Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной
безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с классификацией средств биометрического распознавания.
2. Теоретически ознакомиться с рисками нарушения ИБ при использовании биометрических систем.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

БИОМЕТРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Биометрия – способ распознавания людей по одной или более физическим или поведенческим чертам

Биометрические данные можно разделить на три группы.

Ниже представлена схема-классификация, на которой отображено деление на эти три группы и подвиды-представители технологий биометрии, которые относятся к этим группам (рис. 1).

Рис. 1. Классификация средств биометрии

Физиологические характеристики:

1) Отпечатки пальцев: теория об их уникальности была выдвинута еще в 1877 году. В наши дни этот признак является одним из самых распространенных и хорошо изученных, практически в каждом современном смартфоне есть датчик отпечатка пальца.

2) Геометрия кисти руки: для такого признака измеряется профиль руки, т.е. объем кисти и пальцев их длина, а также неровности ладони и расположение складок кожи на сгибах фаланг пальцев.

3) Радужная оболочка глаза: чтобы произвести распознавание используется видео захват с камеры с помощью программных средств выделяется область зрачка и самой радужной оболочки глаза. Далее полученное круговое изображение конвертируют в чернобелый прямоугольный формат iris code (подобие QR-кода).

4) Сетчатка глаза: метод основан на распознавании по уникальному рисунку сосудов и капилляров на сетчатке глаза. Сложен с технической точки зрения, может произойти отказ в распознавании в случае изменения рисунка от действия болезни или не правильном положении головы при сканировании.

5) Рисунок вен: бесконтактный способ распознавания, основан на способности гемоглобина крови поглощать инфракрасное излучение. В результате работы такого датчика, получают изображение, где рисунок вен выделен более темным цветом.

6) Лицо: данный вид технологии распознавания делится на два подвида: 2D и 3D распознавание. В основе двухмерного распознавания лежат плоские двухмерные изображения, лица на этих изображениях можно с помощью алгоритмов представить в виде графов со взвешенными вершинами и ребрами. Трехмерное распознавание представляет собой 3D сканирование лица с помощью специальных сканеров.

Психологические характеристики:

1) Почерк и анализ рукописной подписи: применяют теорию нейронных сетей. На сегодняшний день это одна из самых лучших технологий для распознавания графических образов. Конкретно для этой задачи используют обучение нейронной сети с учителем.

2) Голос и ритм речи: голоса людей сильно отличаются и это обусловлено как физиологическими отличиями (в росте, весе, поле, возрасте, размере рта),

так и психологическими (в громкости, скорости, высоте, в особенности дыхания). Современные системы распознавания учитывают все эти факторы, разбивают запись голоса на «голосовые отпечатки» и далее производят их оцифровку и сравнение.

3) Скорость и особенность печати на клавиатуре: основными отличительными характеристиками клавиатурного ввода является период удержания клавиши нажатой и время паузы между нажатиями клавиш. Этот метод сложно применить по отношению к малоопытным пользователям, т.к. их клавиатурный почерк еще недостаточно полностью сформирован. В случае обычного пользователя на эти характеристики может повлиять психологическое состояние (усталость, возбужденность или внешние отвлекающие факторы).

4) Походка: каждый человек передвигает свое тело в пространстве уникально, так как он не просто переставляет ноги, хотя их тоже можно переставлять по разному (например, человек может быть пожизненно хромым или переставлять ноги с разной скоростью), но и дополнительно совершает различные движения, одними из таких движений являются взмахи руками с разной интенсивностью. Это дает возможность для каждого индивида выделить паттерны-образцы походки и на их основе распознать человека. К биохимическим характеристикам на данный момент времени можно отнести только один способ распознавания – ДНК (он же генетическая дактилоскопия). В любом биоматериале человека есть ДНК и по ее отличительным особенностям, выявляемым при анализе, можно однозначно определить индивида.

В отличие от прочих методов аутентификации биометрический метод – вероятностный, так как существует шанс, что биометрические

характеристики двух людей могут совпасть. Поэтому введены следующие понятия:

FAR (FalseAcceptenceRate) – процентный порог, определяющий вероятность того, что один человек может быть принят за другого (коэффициент ложного доступа, также именуется «ошибкой 2 рода»). Величина 1-FAR называется специфичность.

FRR (FalseRejectionRate) – вероятность того, что человек может быть не распознан системой (коэффициент ложного отказа в доступе, также именуется «ошибкой 1 рода»). Величина 1-FRR называется чувствительность.

Необходимо учитывать вероятность возникновения ошибок FAR/FRR: искусственным снижением уровня «требовательности» системы (FAR), как правило, уменьшают процент ошибок FRR и наоборот. Критичным минимальным порогом для FAR специалисты называют шанс допуска постороннего в 10^{-5}, что соответствует десятеричному 4-разрядному коду. Для FRR всё зависит от пропускной способности системы. В масштабах небольшого предприятия минимальным порогом может быть 10^{-2}, то есть 1 отказ в доступе из 100 легитимных попыток, для более нагруженных систем этот параметр более критичен. В целом отказ в доступе менее опасен, чем ошибочный доступ стороннего субъекта.

Для повышения точности и надежности распознавания и уровня безопасности системы применяют комбинированные биометрические системы, использующие несколько биометрических характеристик. Например, систему распознавания папиллярных линий на пальцах рук можно сочетать со сканированием руки. Подделать целый ряд биометрических характеристик – сложная задача. Также для повышения комбинируются варианты аутентификации с помощью биометрии и сторонних устройств.

Риски нарушения ИБ при использовании биометрических систем и существующие рекомендации по их предотвращению.

В общем случае можно выделить следующие типы рисков:
1) Риски, которые могут возникать при сборе биометрических данных. Такими рисками являются угроза нарушения целостности в случае подмены или удаления биометрических ПД сотрудниками, занимающимися сбором этих образцов и занесением их в систему, угроза нарушения конфиденциальности в случае раскрытия, передачи образцов третьим лицам.
2) Риски, которые связанные с нарушениями при неправильной обработке/хранении биометрических ПД. Сюда, например, можно отнести хранение подобных данных в незашифрованном виде на носителях данных, не соответствующих требуемым степеням защищенности.
3) Риски, которые могут возникать в ходе процесса биометрической верификации в случае успешной подделки злоумышленником образцов биометрического материала.

Для предотвращения таких рисков, рассмотрим рекомендации, которые дает ЦБ РФ в следствии введения системы Единой Биометрической Системы (ЕБС):
1) Рекомендуется использовать средства криптографической защиты информации (СЗКИ), имеющие подтверждение требований надежности. Этот пункт может относится к минимизации второго риска.
2) Рекомендуется размещать объекты, связанные с обработкой биометрических ПД в отдельных сегментах вычислительных сетей. Доступ к отдельному сегменту проще контролировать, а значит лица, не имеющие на то доступ, легко его не получат. Этот пункт минимизирует первый риск.
3) Рекомендуется уведомить сотрудника, занимающегося обработкой и сбором биометрических данных, о протоколировании его действий и об

ответственности за нарушение законодательства РФ в данной сфере. Данный пункт также минимизирует первый риск.

4) Рекомендуется исключить возможность хранения биометрических персональных данных физических лиц на рабочем месте, предназначенном для сбора/обработки биометрических ПД, после завершения регистрации биометрических ПД. Это минимизирует третий риск, так как один из каналов, для утечки образцов с целью их подделки, будет закрыт.

5) Использовать средства электронной цифровой подписи (ЭЦП) для гарантии контроля целостности собираемых биометрических данных.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомилась с классификацией средств биометрического распознавания, рисками нарушения ИБ при использовании биометрических систем, а также рекомендациями по их предотвращению.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1) Чурилин, Г. Н. Биометрия в информационной безопасности / Г. Н. Чурилин, Е. А. Максимова // НБИ технологии. – 2019. – Т. 13. – № 4. – С. 30-36. – DOI 10.15688/NBIT.jvolsu.2019.4.4.

2) Черноусова, Т. Г. Биометрия и аутентификация / Т. Г. Черноусова // Мир современной науки. – 2017. – № 3(43). – С. 20-24. Лукашов, И. В.

3) Белов, В. Н. Биометрия в России / В. Н. Белов, М. О. Акимкин // Advanced Science. – 2020. – № 4(19). – С. 36-41. – DOI 10.25730/VSU.0536.20.038.

4) Состояние и перспективы биометрии / И. В. Лукашов // Мир измерений. – 2009. – № 3. – С. 27-32.