сотрудников к работе, поскольку в за свой труд они получают гораздо больше, чем ежемесячная заработная плата.

Обобщая вышеизложенное, хочется отметить, что каждая компания в праве разрабатывать локальные показатели для оценки эффективности работы своих сотрудников, которые будут учитывать опыт работы, количество успешно закрытых проектов, участие в каких-либо конференциях и т. д. Нормативные значения результатов оценки эффективности работы персонала для каждой организации венчурной отрасли будут отличаться, поскольку необходимо учитывать продолжительность и специфику. Считаем, что систематический анализ работы сотрудников наряду с расчетами показателей экономической эффективности сможет также дать представление о перспективах успешного развития компании.

Библиографические ссылки

1. Инновационная деятельность и венчурный бизнес: научно-методическое пособие / И. В. Войтов [и др.]. Минск : ГУ «БелИСА», 2011. 188 с.

2. Осипова Т. Е. Анализ лучших мировых HR-практик: успехи их применения в России // Управление развитием персонала. 2013. № 2. С. 90–94.

3. Киселев А. В. Обзор ключевых трендов, меняющих сферу управления персоналом // Управление развитием персонала. 2017. № 4. С. 246–258.

УДК 004.056.5

ПРИМЕНЕНИЕ БИОМЕТРИЧЕСКИХ СИСТЕМ В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Р. Лесько[1)], А. Г. Зданевич[2)], Л. О. Кулакова[3)] (*научный руководитель*)

[1)] *студентка, Брестский государственный технический университет, Брест, Республика Беларусь, f0003712@g.bstu.by*

[2)] *студентка, Брестский государственный технический университет, Брест, Республика Беларусь, f0003707@g.bstu.by*

[3)] *старший преподаватель, Брестский государственный технический университет, Брест, Республика Беларусь, lejla67@mail.ru*

В этой статье описывается надежность биометрических систем, которые используются для идентификации людей. Биометрические технологии предлагают очень привлекательные решения для обеспечения безопасности. Несмотря на риски, системы удобны и их трудно дублировать. Кроме того, эти системы будут продолжать развиваться в течение очень долгого времени в будущем. Вы можете думать о собственном теле как о ключе к открытию безопасных зон.

Ключевые слова: биометрия; информационная безопасность; технология; распознавание.

USE OF BIOMETRIC SYSTEMS IN INFORMATION SECURITY ISSUES

A. R. Lesko[1)], A. G. Zdanevich[2)], L. O. Kulakova[3)] (*supervisor*)

[1)] *Student, Brest State Technical University, Brest, Republic of Belarus, f0003712@g.bstu.by*

[2)] *Student, Brest State Technical University, Brest, Republic of Belarus, f0003712@g.bstu.by*

[3)] *Senior Lecturer, Brest State Technical University, Brest, Republic of Belarus, lejla67@mail.ru*

This article describes the reliability of biometric systems that are used to identify people. Biometric technologies offer very attractive security solutions. Despite the risks, the systems are user-friendly and difficult to duplicate. Moreover, these systems will continue to evolve for a very long time to come. You can think of your own body as the key to opening safe areas.

Keywords: biometrics; information security; technology; recognition**.**

С появлением Интернета и возможности установления соединений стало необходимо проложить виртуальные границы с фактическими границами. Информация стала самым важным ресурсом эпохи, а Интернет сделал возможным доступ к ресурсам, которые могут иметь решающее значение для безопасности.

Биометрия – это измеримые человеческие черты, характеристики или поведение, которые используются для проверки личности. К примеру, анализ отпечатков пальцев, распознавание лица и голоса – все это формы биометрических технологий, но лишь наиболее узнаваемые варианты. Исследователи утверждают, что форма уха, то, как кто-то сидит и ходит, уникальные запахи тела, вены на руках и даже искажения лица являются уникальными идентификаторами. Эти черты в дальнейшем определяют биометрию. Биометрия имеет преимущество перед другими методами идентификации личности, поскольку для распознавания используются характеристики, присущие людям [1].

Сегодня биометрическая безопасность – один из наиболее достоверных методов, использующийся для идентификации человека. Системы или механизмы, основанные на биометрической безопасности, хранят характеристики человеческого тела, которые не меняются в течение жизни человека. К ним относятся отпечатки пальцев, текстура глаз, голос, рисунки рук и распознавание лиц.

Биометрические системы безопасности часто сочетают идентификацию и аутентификацию, однако эти функции не совпадают. При биометрической идентификации система идентифицирует человека путем поиска совпадения по шаблонам всех пользователей в базе данных. С другой стороны, при биометрической аутентификации система определяет, является ли человек тем, кем он себя называет: система проверяет личность человека, сравнивая записанные биометрические данные с шаблоном, хранящимся в базе данных.

С большой скоростью возрастает значение биометрической безопасности в современном обществе. Физические параметры уникальны и неизменны, поэтому биометрическая идентификация личности способна заменить или дополнить системы паролей для телефонов, компьютерной техники и зон ограниченного доступа.

После сбора и сопоставления биометрических данных, характеристики тела человека предварительно сохраняются в биометрической системе безопасности или сканере, доступ к которым имеет уполномоченный персонал. Когда человек входит в учреждение или пытается получить доступ к системе, биометрический сканер оценивает его физические характеристики, которые сопоставляются с сохраненными записями. Если совпадение обнаружено, человеку предоставляется доступ.

Биометрические сканеры – это оборудование, используемое для считывания биометрических данных для проверки личности. Эти сканирования сопоставляются с сохраненной базой данных, чтобы подтвердить или запретить доступ к системе. Другими словами, вы можете рассматривать собственное тело как ключ к открытию безопасных зон.

Одни формы биометрии популярнее других из-за их доступности или высокого уровня точности. Самыми распространёнными формами биометрических систем безопасности являются, [2]:

- распознавание лица;
- распознавание радужной оболочки глаза;

- распознавание сетчатки глаза;
- отпечаток пальца;
- распознавание голоса;
- распознавание вен;
- геометрия рук.

При распознавании лиц используются сгенерированные компьютером фильтры для преобразования изображений лиц в числовые выражения, которые можно сравнивать, чтобы определить их сходство. Для создания фильтров используются искусственные нейронные сети для обработки данных.

Распознавание радужной оболочки глаза – метод биометрической идентификации, который использует математические методы распознавания образов на видеоизображениях одной или обеих радужных оболочек глаз человека. Образцы уникальны, стабильны и видны с некоторого расстояния.

При сканировании радужной оболочки глаза измеряются уникальные узоры радужной оболочки, цветные круги в глазах людей. Биометрические сканеры распознавания радужной оболочки глаза освещают радужную оболочку невидимым инфракрасным светом, чтобы уловить уникальные узоры, невидимые невооруженным глазом. Сканеры радужной оболочки глаза обнаруживают и исключают ресницы, веки и зеркальные отражения, которые обычно блокируют части радужной оболочки. Конечный результат – это набор пикселей, содержащий только радужную оболочку. Затем анализируется образец линий и цветов глаза, чтобы извлечь образец, который кодирует информацию в радужной оболочке глаза.

Отпечатки пальцев часто используется благодаря доступности, безопасности и точности. Сканер создает цифровое изображение отпечатка, а компьютер при помощи программного обеспечения превращает мелкие детали в код, который сравнивается с базой данных.

Системы проверки голоса отличаются от систем распознавания голоса, хотя их часто путают. Распознавание голоса – это процесс распознавания того, что говорит человек, тогда как проверка голоса – распознавание того, кто это говорит.

Распознание вен – вид биометрии, использующийся для идентификации людей по уникальному рисунку вен на ладони или пальце.

Геометрия руки основывается на структуре ладони и пальцев, включая ширину пальцев в разных местах, длину пальцев, толщину области ладони и т. д. Хотя эти измерения не всегда различимы среди людей, геометрия руки может быть очень полезной для проверки личности.

Биометрические системы безопасности возникают во множестве областей, включая бизнес, банковское дело и денежно-кредитную безопасность.

Популярны биометрические системы безопасности для банков. Множество банков, имеющие мобильные приложения, позволяют пользователям проходить аутентификацию при помощи биометрических данных, таких как распознавание лиц, сканирование отпечатков пальцев и голосовая проверка. Мульти факторная аутентификация в комбинации с биометрией способна гарантировать практически непреодолимую степень защищённости.

Сегодня многочисленные компании устанавливают системы контроля доступа, а также учета трудового времени, которые содержат биометрическую аутентификацию.

Биометрическая безопасность платежей интегрирована в процессы авторизации транзакций и на текущий момент включает, в большинстве своем, сканирование отпечатков пальцев.

Защита информации создается с учетом особенностей информационных систем и реализуется комплексом согласованных организационных и технических мероприятий, подкрепленных соответствующими управленческими решениями. Для создания системы защиты информации, в первую очередь, разрабатываются процессы защиты информации и только во вторую очередь разрабатываются и внедряются программно-аппаратные комплексы системы защиты, которые служат для обеспечения процессов защиты информации.

Создание системы безопасности – важнейшее звено в последовательной серии решений по информационной безопасности. Первым и наиболее важным вопросом при создании системы информационной безопасности является оценка требований безопасности, а также идентификация критически важных для безопасности информационных ресурсов защищаемой информационной системы [3].

Развитие информационных технологий привело к модификации старых и появлению совершенно новых форм преступности, связанных с использованием компьютерной информации и различных компьютерных систем. Уголовный закон Беларуси устанавливает ответственность за ряд преступлений против информационной безопасности.

Библиографические ссылки

1. Что такое биометрическая безопасность и почему она имеет значение сегодня : [Электронный ресурс]. URL: https://recfaces.com/articles/biometric-security (дата доступа: 17.10.2021).

2. Технологии биометрической идентификации : [Электронный ресурс]. URL: https://www.tadviser.ru/-index.php/Статья:Технологии_биометрической_идентификации (дата доступа: 17.10.2021).

3. Экономическая безопасность Республики Беларусь : [Электронный ресурс]. URL: https://www.nbrb.by/bv/articles/10866.pdf (дата доступа: 17.10.2021).

УДК 004.652+330.123.6 / JEL D83, L84, L86

СТРАТЕГИИ ПРЕДПРИНИМАТЕЛЬСТВА В СФЕРЕ ГОСТЕПРИИМСТВА В УСЛОВИЯХ ПАНДЕМИИ COVID-19

А. О. Лещенко[1)], Л. Б. Демидчук[2)] (*научный руководитель*)

[1)] *студент, Львовский торгово-экономический университет, Львов, Украина, ulskvo.ua@mail.ru*

[2)] *доцент, Львовский торгово-экономический университет, Львов, Украина, ludalv.ua@gmail.com*

Исследованы актуальные вопросы информационной сервизации в системе услуг индустрии гостеприимства во время процессов трансформации ее инфраструктуры и требований к организации и особенностей предоставления в условиях кризиса во время пандемии COVID-19. Рассмотрен процесс перестройки под цифровые технологии предпринимательских процессов, когда актуальным становится элемент принятия делового решения по инвестициям, включая приобретение нужного программного обеспечения, технического перевооружения и обучения персонала, развитие на предприятии диджитального способа мышления; предпосылки встраивания информационных услуг и консультаций в материально-вещественное производство и его основания. Исследованы составляющие современных инноваций в индустрии гостеприимства. Сделан вывод, что основными задачами стимулирования инновационной деятельности отрасли индустрии гостеприимства являются: развитие институциональных основ интеграции научной, инновационной, производственной сфер; преобразования научной составляющей в активный фактор накопления инновационного потенциала этой отрасли; формирование ее эффективной инновационной инфраструктуры.