Безопасность ЕБС и её элементов. Обзор рисков и перспективных направлений улучшения систем персональной аутентификации

Антти Суомалайнен

Во второй части статьи приведён краткий обзор других существующих на сегодняшний день основных типов квантовых компьютеров:

- **квантовые адиабатические вычислители (Adiabatic Quantum Processing Unit);**
- **вычислители с квантовым отжигом (Quantum Annealing Processing Unit – QAPU);**
- **вариационные квантовые вычислители (Variational Quantum Eigensolvers);**
- **вычислители собственных значений с квантовым отжигом (Quantum Annealer Eigensolver – QAE).**

Традиционные методы аутентификации для компьютеров и сетей – пароли, коды, карты доступа, которые можно передать другому лицу, – устарели как небезопасные и неэффективные для персональной идентификации. На этом фоне биометрическая аутентификация кажется идеальным решением проблемы. Существует несколько видов биометрической аутентификации, в том числе сканирование сетчатки глаза, распознавание лица и аутентификация по отпечатку пальца – самый распространённый вид. Отпечатки пальцев человека уникальны, и принято считать, что по ним можно идентифицировать человека. Однако всё, что касается однофакторной аутентификации, в наше турбулентное время подлежит квалифицированному анализу и обоснованной критике, как не обеспечивающее полной надёжности. Последовательно рассмотрим эти риски.

Так, с помощью технологии трёхмерной печати – по заранее полученному слепку – можно создавать копию отпечатка пальца. По мнению специалистов, несанкционированными методами копирования достигают 80% успеха при использовании поддельных отпечатков из историй, когда биометрические датчики были обмануты хотя бы однократно. И это, разумеется, существенные риски для ЕБС и современного электронного оборудования, задействованного в устройствах безопасности. Одна из проблем для клонирования отпечатка – это формы. Форма должна иметь в точности те же размеры, что и эталон (оригинал отпечатка); при отклонении в размере даже 0,1 мм форма непригодна для использования. Но, в принципе, изготовить реплику отпечатка вполне посильно даже в бытовых условиях. Похожим методом много лет изготавливают реплики печатей. На рис. 1 представлена иллюстрация папиллярных линий на пальце.

Рис. 1. Иллюстрация папиллярных линий на пальце

Риски аутентификации по отпечатку пальца

Дермальные гребни отпечатков пальцев имеют ширину примерно 500 микрон и глубину 20–50 микрон. Гряды и впадины папиллярного рисунка имеют разные эхосигналы, поэтому сканер преобразует «рисунок» пальца в псевдоизображение в цифровом виде. Сегодня в устройствах биоидентификации по отпечаткам используют три основных типа датчиков: оптические, ёмкостные и ультразвуковые. Все они имеют преимущества и недостатки, однако с точки зрения безопасности доступа и аутентификации между ними нет явного преимущества. Так, активные ёмкостные датчики-сканеры считывают папиллярный рисунок кожи пальца по проводимости его линий. Основными ограничениями для ёмкостных датчиков являются разрешение и проводимость. Эффективность оптического метода зависит от качества «оптики», стекла рабочей поверхности сканера и непосредственно датчика. «Картинка» захватывается матрицей элементов с зарядовой связью CCD и элементов CMOS, затем преобразуется в изображение в оттенках серого (до 16).

Все типы сканеров мы рассмотрели в статье «Датчики-сканеры отпечатков пальцев в устройствах биоидентификации. Обзор и перспективы» в № 9, 2022 «Современная электроника», но добавлю ещё один условный «минус» оптического метода сканирования. Незаметный отпечаток пальца остаётся на рабочей поверхности сканера – на стекле и может быть использован повторно. Другая сложность в том, чтобы отличить настоящий палец от качественной реплики. Об этом мы подробно поговорим далее.

Ультразвуковые датчики для сканеров излучают импульс УЗЧ, эхо которого считывается приёмным узлом и далее поступает на сервер. Ёмкостный метод с применением активных и пассивных датчиков-сканеров, хоть и считается самым популярным, также сравнительно легко обмануть имитированным отпечатком или скрытым отпечатком на поверхности сканера. Нажимной метод характеризуется сравнительно низкой чувствительностью, неспособностью отличить настоящий палец от имитации, подверженностью повреждениям из-за чрезмерных прилагаемых усилий и практически не используется в современных ЕБС, связанных с аутентификацией человека. Тем не менее есть направление деятельности, которое сегодня активно разрабатывается, – биоакустическая аутентификация, связанная с прикосновением пальца к рабочей поверхности сканера и последующим анализом вибраций. Тут понятия «нажимной» и «вибрационный» некоторым обра-

зом коррелируют. Подробно об этом в заключительной части статьи.

Итак, один из основных рисков обмана сканеров отпечатков систем безопасности в ЕБС – изготовление и применение клонированного (поддельного) отпечатка, получить который можно разными способами. Злоумышленник получает отпечаток пальца жертвы, затем готовит поддельный отпечаток-реплику. Причём реплику отпечатка можно создать из нескольких частей (сканированных изображений) одного и того же пальца. Как известно, сбор отпечатков происходит на таможне, на границе и в других случаях. В несанкционированном сценарии сбор биоматериала может осуществляться через фотографирование отпечатка на стакане, бутылке, даже дверной ручке – если отпечаток качественный. Перед фотографированием отпечаток можно дополнительно «подсветить», обработав кисточкой с графитовым или алюминиевым составом (порошком). Несанкционированным способом снять отпечаток можно во многих случаях: человек спит, в больнице, без сознания, нетрезв, иным образом не контролирует свои действия. Существует и несколько альтернативных фотографированию способов, в частности, слепок с помощью липкой ленты и др.

Далее рассмотрим популярный метод репликации отпечатка при несанкционированном клонировании.

Методы репликации при несанкционированном клонировании

Как происходит несанкционированное клонирование отпечатков? Аналог отпечатка пальца создают с оригинала. Растровое изображение получают со сканера отпечатков пальцев, причём подходит даже «бюджетный» вариант считывателя, к примеру, PUPPY SONY, приобретённый через почтовый сервис китайского оператора. Или иной сканер с подключением UART либо совмещённый с преобразователем CP2102 USB в TTL, адаптированный с ПК или Arduino UNO. Пример сканера представлен на рис. 2.

Трёхмерный макет создают с помощью ПО для трёхмерной цифровой структуры. Затем с помощью ультразвукового 3D-принтера изготавливают форму из мягкого материала, которая затем затвердевает. В некоторых источниках (список в заключении) описывается апробированный метод изготовления формы из желатина и др. ингредиентов, но есть и другие варианты – пластилин, смесь силикона и тканевого клея, глина для скульптурных работ и др. «Скульптурная» глина имеет твёрдость при комнатной температуре, но становится мягкой и даже жидкой, если температура достаточно высока. Это условие выполняют, нагревая материал электрическим феном. Чем выше точность УФ-принтера, тем качественнее реплика отпечатка. Уже при точности (разрешении) в 25 мк, что даёт даже современное бытовое оборудование, сия небезупречная задача решается просто.

Отвердение копии в УФ-камере в течение нескольких минут обязательно, чтобы устранить токсичность смолы и закрепить форму. Прямое воздействие ультрафиолета изменяет размер объекта из-за сжатия смолы. Поэтому пресс-форма из смол – не лучший выбор, и для её создания лучше использовать альтернативный материал без ограничения втягивания.

Аутентификация по отпечатку пальца широко используется на многих типах устройств. Однако надёжность не на всех устройствах одинакова. Трудности проиндексировать большую базу данных до сих пор считаются актуальными и требуют ускорения процесса анализа отпечатков. Также заинтересованные лица должны знать, что безопасность аутентификации по отпечатку пальца несовершенна, несмотря на распространённые мифы. В зависимости от конкретного профиля угроз использование аутентификации по отпечатку без комплекса других мероприятий и методов может быть нецелесообразным.

Особенности распознавания по рисунку вен рук

Распознавание аутентификационных признаков по рисунку вен руки – условно новая технология, пока не получившая бытового распространения, но применяется в ЕБС как комплексный элемент системы безопасности, повышающий её надёжность. На примере изученного биометрического считывателя вен ладони PalmVein метод не требует условно дорогостоящего оборудования в сравнении с устройствами распознавания по геометрии лица или радужной оболочке. Однако в перспективных разработках необходимо учитывать следующие

Рис. 2. Сканер PUPPY SONY, адаптированный к ПК

факторы. Не только рисунок вен, но и хиромантические линии как признак индивидуальности (линия жизни и др.) являются идентификационным признаком. По ним легче всего предварительно идентифицировать и отобрать несколько человек. Также, несколько худшим из-за возрастных изменений, идентификационным признаком является форма и размер ладони. Тем не менее комплексное сканирование в ЕБС отпечатка каждого из 5 пальцев со всеми 14 фалангами с отпечатком ладони уместно использовать для окончательного подтверждения личности. Это всё уже использовалось в дактилоскопии – именно в таком полном варианте отсканированных идентификаторов; сегодня речь о том, чтобы ввести эту систему в электронный вид и практику, как дополнительный элемент надёжности в ЕБС.

Риски и перспективы для ЕБС с методом распознавания лиц

В коммерческих (негосударственных) условиях применения задачи аутентификации специфичны. «Know your customer?» – такой вопрос волнует руководителей и менеджеров торговых сетей – для последующего маркетинга и аналитической работы на развитие: нужно знать образ и запросы «своего» покупателя из сопоставления хэш-кода лица и покупок. Отсюда, из этого опыта, можно понять перспективный принцип идентификации покупателя в магазине. Это кроме актуальных вопросов безопасности и не теряющей актуальности борьбы с кражами в торговых залах. Реализуется «коммерчески-торговый» вариант с

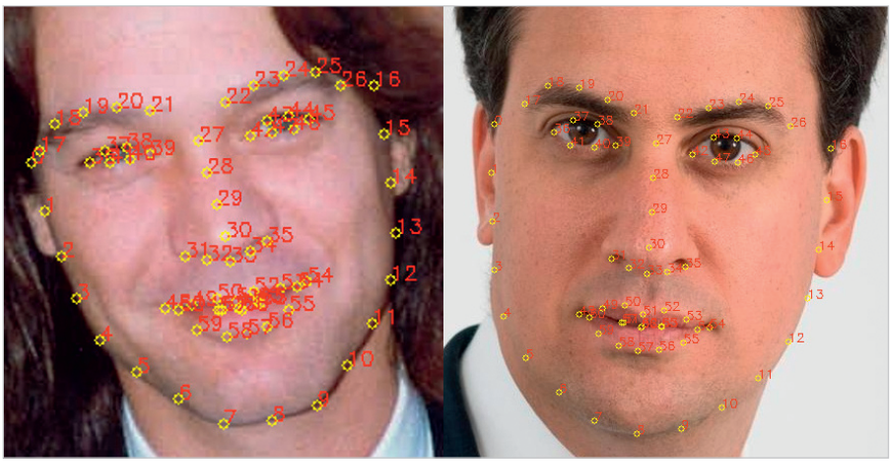


Рис. 3. Иллюстрация лиц и типичных «точек» для идентификации

помощью пополняемой базы покупателей и их фотоизображений. Пока база данных несколько тысяч человек, всё это работает. Но в крупных торговых сетях этого уже недостаточно. Интересный опыт дают «бескассовые магазины», где огромное число камер (распространены в США, Германии и в др. странах). Отслеживают покупателей в торговом зале – от выбора покупки до её оплаты на терминале. Для этого системе требуются не только «картинка» и лица, но и аутентификация по другим признакам, что и делается у терминала оплаты. Это биоидентификация по отпечаткам пальцев и (или) фронтально установленная видеокамера с ИК-подсветкой. По этим признакам покупатель распознаётся в базе. Однофакторный метод аутентификации через дисконтную или банковскую карту, которую можно передать другому лицу, не даёт удовлетворительных результатов, если предполагать, что задача коммерческой сети всё-таки в том, чтобы проводить персонализированный и общий маркетинг покупок, интересов и запросов, а не только решать вопросы безопасности и работать против краж.

Рисковые варианты корректного считывания по геометрии лица сводятся к изменению геометрии лица – формы и типичных точек расположения основных идентификационных признаков (нос, глаза, рот), а также расстояний между ними. На рис. 3 представлен вид с лицами и типичными точками для идентификации.

Так, нанесение маркером стрелок, фигур, дополнительных «зрачков» и «глаз» не исключает корректного считывания признаков, но затрудняет эту функцию. В этой связи надёжная работа ЕБС зависит от двух факторов: качества камер и качества ПО, ибо именно на сервере (ПК) анализируется и сравнивается полученное с видеокамер изображение. Принудительное нанесение на лицо новых «элементов» изменяет координаты оригинального признака на несколько миллиметров, и этого достаточно для того, чтобы точность распознавания значительно снизилась, для сбоя работы ЕБС с устаревшим ПО и выдачи ошибок. Такая ЕБС распознает и условного злоумышленника, и одновременно ещё сотни человек. Надо также принять во внимание, что в будущем, в связи с развитием высоких технологий и психологически обоснованного вектора социопатии в обществе, такие риски, связанные с попытками «уйти от камер» даже законопослушных граждан, будут нарастать. Отсюда на сегодняшний день понятно, что для корректного анализа идентификационных данных человека на сервере нужно идти путём наращивания числа признаков. По условной аналогии с базой отпечатков пальцев, куда рекомендую включать, кроме папиллярного рисунка пальцев, и ладони, и фаланги пальцев, в части сканирования геометрии лица необходимо в оригинальном признаке делать несколько «эталонов» лица – вблизи, вдали, анфас, профиль, в фокусе каждый конкретный признак (нос, рот) и его элементы. Речь идёт о разделении признаков и «картинок» по ним. Пока же (на сей день) абсолютная точность распознавания ЕБС человека по геометрии лица недостижима.

Так, близнецы вызовут ложно-положительные сигналы, но тут проблема не в несовершенстве алгоритма распознавания, а в реальной похожести. А с ложно-положительными «тревожными» сигналами, вызванными несовершенством алгоритма, борются статистическим методом. Если в поле зрения массива видеокамер есть разыскиваемое лицо, оно будет «опознано» по картинкам с нескольких, а не с одной камеры. И чем большее количество камер даст картинки, проанализированные сервером как «изображение поиска» из соответствующей базы, тем меньше вероятность ошибок ЕБС и системы поиска. Есть уже реализованные пути решения на примере системы видеоконтроля в метро. Перед станциями, в вестибюлях, на эскалаторах, на платформах и даже на турникетах установлены камеры видеонаблюдения. Корректность работы ЕБС в данном случае прямо зависит от качества камер (оптики камер и электронного АЦП системы) и их количества. Важный элемент работы реальных систем аутентификации: возможность массового сравнения многих изображений одного лица. Отслеживание движения дополняет распознавание лиц. Человек заходит в вестибюль метро (2-3 картинки, к примеру), потом спускается по эскалатору (еще 3-4 картинки) и проходит к платформе (2-3 картинки). С помощью реализованных в поисковой системе алгоритмов она «ловит» человека с помощью полученных изображений – на совпадение, к примеру, с паспортной фотографией разыскиваемого – статистическим методом. В этом смысле интересны перспективы аутентификации в движении.

Аутентификация в движении

Скорость потока пешеходов или пассажиров в переходе отслеживают по характерным лицам, что удобно делать на полупустой улице. Последовательность появления одного лица в массиве видеокамер легко предсказывается, а отслеживать можно по комбинации цветов одежды. При больших скоплениях людей, в частности, на вокзалах, в транспорте, в метро алгоритмы поисковой системы несовершенны. Для поиска человека по картинке с видеокамер открываются две задачи: «tracking» и «reindentification». Но это уже частные случаи. Именно поэтому количество видеокамер (практически везде) систематически наращивают, а не снижают (см. источники к публикации). Нередко в транспортной инфраструктуре большое количество видеокамер, сконцентрированных на одной площад-

ке потолка, «смотрят» в залы. Эти задачи решаются по-разному, 100% достижения эффекта нет, и есть как технические проблемы, так и несовершенства, связанные с человеческим фактором. Если не лениться и исследовать запросы и ожидания крупных транспортных корпораций, к примеру «Мосгортранс», окажется, что и они в поиске более совершенного решения относительно того, как считать пассажиров – по головам вручную или с помощью автоматизированной системы. Проблемное поле: во-первых, такие системы дороги – это понятно; во-вторых, они не дают гарантии, но всё же способствуют учёту с некоторой долей погрешности.

А как работает поисковая программа, спонсированная государством? Ведь только в Петербурге и Ленинградской области примерно 30 000 человек в базе розыска. Моделируем ситуацию с поиском «лица» в многотысячном потоке пассажиров метро. В среднем человек проводит на станции, скажем, 5 минут. При заходе на станцию, и даже перед ней «картинка» уже считывается камерами видеонаблюдения. Если есть «срабатывание» по изображению с камер на «лицо», прошедшее в вестибюле, то дальнейший поиск осуществляется не только в сравнении с паспортной фотографией, имеющейся в базе поиска, но и с изображением, полученным в разных ракурсах с других камер этой же станции. Причём система уже давно работает автоматически, правда, это не говорит о том, что нет операторов, контролирующих видео в реальном режиме. Но оператор не может и не будет фактически делать «траки» в массиве из нескольких тысяч изображений. Эта кропотливая работа возможна только в весьма неординарных случаях. Итак, на условной станции 50 камер. Поток пассажиров в среднем 60 000 в день. Камеры установлены в разных местах и под разным углом. В результате и к примеру, если на 10 из 50 камер опознался разыскиваемый, идёт команда на полицейский пульт. Если обнаружен на одной-двух камерах – это допустимый вариант «ошибки».

Не надо искать (по дисплеям от видеокамер) человека в толпе. Достаточно знать, что с момента обнаружения подозреваемого в вестибюле и его входа до условной потери человека системой наблюдения есть запас времени в 10 минут: 4-5 минут – спуск по эскалатору, остальное время прохода до и после него. После вестибюля перед потенциальным разыскиваемым ещё десятки камер. Допустим, «лицо» опознано как разыскиваемое на эскалаторе – по камерам № 10 и № 16, а видео с камер № 6–9, № 11–15 (часть из них «смотрит» не фронтально) не распознано. Тогда оператор занимается этим «лицом» плотно, но не ищет его в толпе, а ждёт отклик системы – сколько ещё видеокамер «распознают» лицо, и где они расположены.

Специалисты осведомлены, что камеры сами по себе не распознают. Распознаёт алгоритм, который работает на серверах по изображениям с камер. Ошибка не будет зависеть от камеры, а только от ракурса и условий съёмки. В движении ракурс и условия будут каждый раз разными. Но возможно уменьшить количество ошибок теперь даже с условно старым оборудованием. В условно больших помещениях устанавливают шлюзы на манер концентрации людского потока типа «воронка». В «шлюзах» обеспечивают хорошее освещение – одно из условия качественной картинки с видеокамеры. Оборудование (видеокамеры) устанавливают с хорошим разрешением и с настраиваемым функционалом, в том числе функцией zoom. Этот комплекс мер повышает качество видеокартинки, а совершенствование ПО – качество анализа и аутентификации; таков путь совершенствования системы безопасности на основе ЕБС.

Перспективные методы и решения

Модель программного описания отпечатка основана на описании топологии, поэтому появляется независимость от деформаций отпечатков и от масштаба. В некоторых базах, содержащих больше 2 тысяч отпечатков, могут фиксироваться ложные срабатывания. Их вероятность примерно 1 ошибка на 1000 случаев. При использовании двух отпечатков – одна ошибка на 1 000 000 случаев. По статистике ошибок 1% FRR до 0,01% FAR (при приемлемых FRR) считают хорошим показателем.

При серьёзных повреждениях папиллярного рисунка нужно использовать и другие пальцы руки, и альтернативные методы, к примеру, сканирование ладони. Поэтому в современных базах данных регистрируют несколько пальцев. В СКУД и в платёжной (банковской) системе человек заинтересован сам в быстрой и корректной идентификации, поэтому и специальные меры к принуждению его для сдачи оригиналов отпечатков не требуются. Есть коммерческие системы с базой данных в 10 млн эталонных отпечатков. Понятно, что государственные серверы имели сию возможность и ранее – в России в электронном виде базы оцифрованы (не на перфокартах, а адаптированы для ПК) примерно в 2012 году. Если использовалась 10-пальцевая регистрация, дающая 100% результат аутентификации, электронная система решает две задачи: определит, входит ли отпечаток в список из 3-5 настроенных, и корректно определит владельца отпечатка в базе из 10 миллионов.

Биометрия, особенно комплексная и (или) реализованная с применением качественного оборудования на примере трёхфакторной и спектральной идентификации отпечатка, – надёжнее PIN. Теоретически пластик можно заменить цифровым идентификатором – даже номером телефона. А отпечаток пальца при этом будет выполнять функции ПИН-кода. Ещё вариант перспективной аутентификации: отпечаток пальца и тепловая «картина» кровеносных сосудов, а также динамические биометрические признаки, к примеру, рукописный пароль.

Биометрические алгоритмы строятся на обучаемых нейронных сетях, актуален вопрос о взаимодействии разных сетей, ПО и др. Алгоритмы с динамическими биометрическими признаками пока тоже не достигли совершенства. Статистические методы лучше работают на этапе создания ординарного признака, к примеру, отпечатка. Вот почему качество оригинала остаётся важным для всей ЕБС. Действительно, лучше на этапе создания эталона потерять время, чтобы впоследствии обеспечить автоматическую и быструю верификацию.

Предполагается, что зависимость от растительности на лице, причёски не является критичной для распознавания лиц в современных ЕБС. Системы видеоконтроля-нахождения не анализируют причёски и растительность на лице. Даже овал лица некоторые алгоритмы не учитывают, ибо под разными ракурсами одно и то же лицо имеет разные (отличные) профили. Но это не всегда так. На рис. 4 представлен вид автора в маске, исключающей аутентификацию по геометрии лица.

Метод многократно апробирован авторским опытом в 2020–2022 гг. Тут

Рис. 4. Автор иллюстрирует метод, исключающий аутентификацию по геометрии лица

надо для справедливости заметить, что обнаружение такого «лица» в период «масочного режима», связываемого с коронавирусом, не приводило в Санкт-Петербурге к вопросам, уточнениям или задержаниям. И вызывало лишь восторженные взгляды. Однако в настоящей ситуации, когда «масочный режим» отменен, такое «лицо» само по себе, пожалуй, может вызвать вопросы у представителей правопорядка. Впрочем, ношение масок не запрещено, а как определяется маска – до сих пор вопрос полемичный. Поэтому попытки простыми методами аутентифицировать (контролировать) людей алгоритмами, сопоставляя лица с «исключающими шаблонами», приведут к увеличению количества ошибок. К примеру, в известной программе «заменитель лиц» FaceSwap сделана попытка с алгоритмом GAN128 отделить лицо от посторонних предметов, перекрывающих лицо (причёска, пирсинг, руки и т.д.). В этом случае вариант – делать многократное сопоставление шаблонов, то есть совершенствовать ПО. Кстати, современные сканеры отпечатков не то что стекло – мёртвый палец отличают от живого. Однако НТ-прогресс идёт вперед, в соответствии с сентенцией «на каждое действие возможно противодействие» созданных систем безопасной аутентификации уже недостаточно; они должны совершенствоваться постоянно. Как вариант, уместно рассматривать – в числе прочих – биоакустическую аутентификацию как дополнительный способ идентификации.

Биоакустическая аутентификация

Известны акустические методы распознавания голоса с помощью спектральных фильтров, аналитика сигнатур дыхания, а в формате биоакустики анализируется биодинамическая реакция пальца в акустическом спектре. Метод биоакустической аутентификации имеет особенности как в принципе работы, так и в сканирующем оборудовании. При касании рабочей поверхности сканера микровибрации пальца считываются датчиком. Причём индивидуальная форма сигнала сохраняется при разной силе нажатия пальца. Из-за индивидуальных анатомических особенностей сканированный сигнал обладает неповторимостью. Содержит анатомическую информацию о структуре тела, о костной, хрящевой, сухожильной и мышечной ткани, полагается на их геометрию, а также на биомеханические свойства. Преобразованные датчиком в цифровой вид, данные служат для последующего компьютерного анализа и имеют то же значение биоинформации, что и отпечаток пальца, образец голоса, рисунок сетчатки глаза, геометрии лица и др. То есть служит идентификационной характеристикой человека и может использоваться для его аутентификации.

Передача характеристик вибрационных сигналов через кости и ткани пальца осуществляется так: синусоидальный (аналоговый) сигнал поступает на вход преобразователя и передаётся ЗЧ через палец, воспринимается микрофоном, демодулируется с помощью опорного сигнала, фильтруется фильтром НЧ и оцифровывается АЦП микроконтроллера. Для биоакустической аутентификации пользователь помещает палец на сканер со встроенным трансдуцером – передатчиком ЗЧ и акустическим сенсором. Акустический сенсор расположен на 3 мм выше передней дистальной межфаланговой складки, которая является нижним концом дистальной фаланги. Место для прикосновения (воздействия) пальцем имеет значение. Благодаря форме площадки для сканирования место возбуждения и зондирования выбрано так, что сигнал ЗЧ проходит через проксимальную и среднюю фаланги пальца. Передатчик расположен на расстоянии 50 мм от акустического сенсора, полностью покрывая длину средних фаланг пальца.

Выводы

Перспективы развития и совершенствования электронных сканеров отпечатков пальцев мы рассмотрели в статье СЭ № 9, 2022. Практическая эффективность от клонирования отпечатков определяется наличием или доступом к базе биометрических данных или несанкционированным сбором такой информации, а также наличием оборудования для изготовления реплики-слепка-клона. Даже современные электронные микроскопы позволяют измерять микронные различия в отпечатках, а инструменты высокоточной лазерной гравировки помогают этому. При наличии высокотехнологичного оборудования возможности несанкционированного копирования отпечатков возрастают, соответственно, угрозы безопасности пользователям биометрического оборудования увеличиваются. Чем больше ресурсы у такой небезупречной группы сотрудников, тем больший масштаб угроз и рисков можно ожидать. Для рядового гражданина и пользователя биометрическая аутентификация по отпечатку пальца является действенной защитой в быту. Однако для защиты значительных материальных и информационных ресурсов преимущества биометрии по отпечаткам неочевидны из-за рисков качественной имитации отпечатка и обмана сканера, поэтому метод используют в комплексе с другими защитными мероприятиями, в том числе биометрическими, а также систематически совершенствуют оборудование сканеров и ПО.

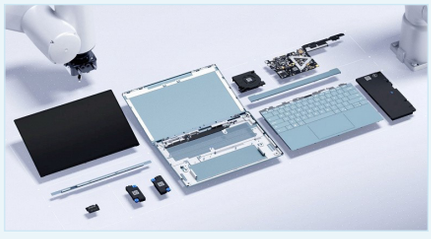
Литература

1. Руководство по проектированию биометрических устройств // URL: https://learn.microsoft.com/ru-ru/windows-hardware/drivers/biometric/.
2. Клонирование отпечатка пальца: миф или реальность? // URL: https://10guards.com/ru/articles/fingerprint-cloning-is-it-real/.
3. Программное обеспечение. Стандартизированные биометрические данные INCITS // URL: https://www.nist.gov/itl/iad/image-group/resources/incits-standardized-biometric-data.
4. *Суомалайнен Антти*. Биометрическая защита: обзор технологии. М.: ДМК Пресс, 2019. 104 с.: ил.
5. *Tsunomi Matsumoto*. Искусственный палец из желатина // URL: http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf.
6. Описание биоакустической подписи в IEEE Transactions on Cybernetics (doi: 10.1109/TCYB.2019.2941281) // URL: https://habr.com/ru/company/vdsina/blog/518294/.
7. Видеоизображение // URL: matthewearl.github.io/assets/switching-eds/landmarks.jpg.
8. *Андрей Кашкаров*. Контрольное видеообозрение россиян // URL: https://xxxx.press/blog/kontrolnoe_video_obozrenie_rossijan/2020-12-28-1075.

НОВОСТИ МИРА

Если все ноутбуки станут такими, то сервисные центры по их ремонту закроются. Dell представила концепт модульного ноутбука Luna

Компания Dell представила Concept Luna – прототип перспективного модульного ноутбука. Тут нет гибкого экрана или большого сенсорного дисплея вместо клавиатуры – наоборот, устройство имеет совершенно стандартный внешний вид. Все самое интересное – внутри.



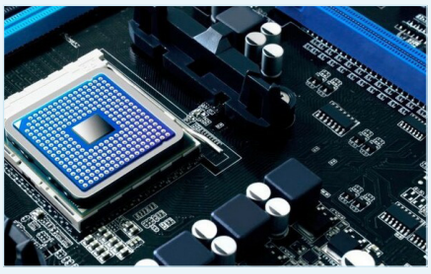
Concept Luna – это практически как конструктор Lego. Устройство состоит из модулей, которые соединяются друг с другом без винтов – всё исключительно на защёлках. Соответственно, для разборки Concept Luna не нужны ни отвёртки, ни какие-то дополнительные инструменты. Разобрать устройство на элементы можно за 30 секунд! Причём это касается и системы охлаждения, и даже матрицы экрана. То есть, например, если разобьётся дисплей, то пользователь сможет заменить его (при наличии новой матрицы) самостоятельно и очень быстро. То же самое касается и апгрейда: достаточно снять модуль системной платы и установить на его место новый. Внешне Concept Luna напоминает обычный 14-дюймовый ноутбук линейки Latitude. Компания отмечает, что это всего лишь концепт, и никакого серийного воплощения его в ближайшем будущем не планируется. Тем не менее, какие-то наработки Concept Luna вполне могут быть реализованы в будущих товарных устройствах Dell.

ixbt.com

Правительство решило открыть во Владимирской области новую ОЭЗ для производителей полупроводников

Председатель правительства Михаил Мишустин подписал постановление о создании особой экономической зоны (ОЭЗ) «Владимир» на территории Киржачского и Александровского муниципальных районов Владимирской области.

В составе ОЭЗ промышленно-производственного типа будет работать ряд предприятий, в том числе по производству электронных компонентов – полупроводников нового поколения, способных в ряде случаев заменить кремниевую электронную компонентную базу, говорится в сообщении правительства.



На сегодняшний день о своём намерении работать в ОЭЗ заявили 13 предприятий.

Размещение в ОЭЗ даёт бизнесу ряд преимуществ. Так, резиденты могут пользоваться налоговыми льготами и таможенными преференциями, а также рассчитывать на снижение арендных платежей.

industry-hunter.com

Путин потребовал запустить новые программы робототехники и авиационных беспилотников

Президент России Владимир Путин призвал запустить новые программы робототехники и авиационных беспилотников.

Об этом в четверг, 15 декабря, сообщает ТАСС.

«Уже просил в наступающем году подготовить и запустить новые программы в области робототехники и авиационных беспилотников. Конечно, обрести технологический суверенитет нельзя, что называется, в один момент, но нужно продолжать системную работу на перспективу», – сказал он на заседании Совета по стратегическому развитию и национальным проектам.

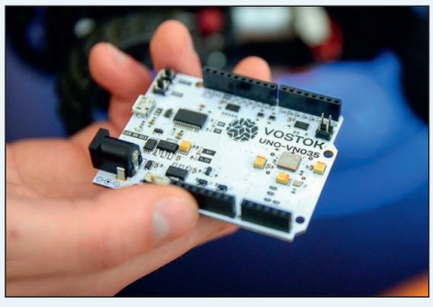
В ноябре глава государства заявил, что в России нужно наращивать усилия по развитию искусственного интеллекта. По словам Путина, в сфере искусственного интеллекта идёт жёсткое соперничество между странами. Вместе с тем РФ обходит их по некоторым направлениям, указал он.

Ранее сообщалось, что в России откроют полигон для беспилотных авиационных систем (БАС), где разработчики смогут проводить лётные испытания дронов. Полигон БАС включает в себя цифровую платформу и собственно лётный полигон, расположенный в районе аэродрома Орловка.

russianelectronics.ru

Российский ответ на платформу Arduino – проект «Vostok» заморожен

Весной этого года в ряде СМИ появилась достаточно любопытная информация о том, что в России идёт разработка отечественной платформы, аналогичной весьма популярной Arduino – работы по ней ведутся в центре «Восток», расположенном во Владивостоке.



Как сообщалось, на данной платформе должны были обучаться порядка 10 миллионов российских школьников – столько учеников планировалось охватить за счёт специальных кружков соответствующей направленности, а также при участии в Национальной техолимпиаде.

Кроме того, новинку должны были использовать и в немного других направлениях – инженерных и робототехнических состязаниях, профильных группах, различных программах образовательной направленности, многочисленных курсах программирования, а также радиоэлектроники. Причем проект официально анонсировали еще летом текущего года с уточнением, что в этом году, 1 сентября, стартует интеграция его в ряд учебных организаций. К сожалению, ни в давно прошедшего 1 сентября, ни даже позднее, данный проект не запустили и даже появились данные, что его заморозили на неуточнённый срок, ссылаясь на какие-то сложности с менеджментом. Хотя в конце прошлого месяца даже предлагалось оформить предварительный заказ на первые экземпляры платы пилотной партии со сроками поставки в ближайшем декабре.

Для справки, платформа с названием Vostok и модельным номером UNO-VN035 по факту совместима с известным во всем мире Arduino и может применять такие же платы расширения, как в Arduino Uno. В основе российского решения лежит отечественный микроконтроллер производства «НИИЭТ» с маркировкой 1921ВК035, построенный на 32-битной RISC-архитектуре.

techcult.ru