В этом номере с вами
Алексей ГИНЦЕ, PR-директор компании «ААМ Системз»
Александр ГОРШКОВ, директор по развитию бизнеса ООО «Айрис Девайсез»
Роман ГОРПИНЧЕНКО, заместитель начальника по проектным продажам Dahua Technology Rus
Андрей ГАБЕЛКО, генеральный директор ООО «ВЗОР Системы Идентификации»
Денис СОКОЛОВ, руководитель группы разработки программного обеспечения Sigur
Андрей ХРУЛЕВ, директор по бизнес-развитию направления биометрических систем группы компаний ЦРТ

Биометрические системы СКУД: проблемы и перспективы

ВОПРОС ДЛЯ ОБСУЖДЕНИЯ

Преимущества и недостатки биометрических СКУД.

Алексей ГИНЦЕ:

– Я бы не стал так ставить вопрос. Это все равно, что спросить о преимуществах и недостатках автомобилей. У «жигуля» и карьерного самосвала слишком разные характеристики, но и то, и другое – машины, решающие разные задачи. Сравнивать их некорректно. Кроме этого нюанса, употребление термина СКУД сильно расширяет тему, поскольку подразумевает помимо считывателей также контроллеры и программное обеспечение. Аппаратная часть чисто биометрической СКУД может быть представлена устройствами, совмещающими считыватель и контроллер в одном корпусе. Думаю, что имеет смысл сузить тематику и сказать пару слов о достоинствах и недостатках биометрических считывателей на основе разных технологий.

Считыватели отпечатка пальца. Огромный пласт рынка биометрических считывателей и наиболее распространенная в настоящее время технология. Сами сканеры могут работать на разных физических принципах (оптические, емкостные и пр.). Недостатки – контактная технология, поскольку необходимо приложить палец к сканеру, на это нужно время, и это не гигиенично. До недавних пор процесс воспринимался некоторыми клиентами негативно, но с распространением технологии на бытовом уровне (смартфоны, ноутбуки и пр.) эта проблема снялась. Достоинства – процесс понятен и привычен для большинства пользователей, цена сканеров и считывателей невысока, огромный выбор устройств разных технологий сканирования и производителей. Технология фактически относится к массовому сегменту рынка.

Сканер рисунка вен пальца или ладони. В сравнении с отпечатком пальца технология более молодая. В силу того, что для распознавания используются внутренние (скрытые) биометрические характеристики, подделка считается более трудной. Некоторые эксперты считают ее альтернативой отпечатку пальца. Недостатки – условно контактная технология (нет прямого контакта со сканером). Условно контактная, поскольку в наиболее распространенных типах считывателей требуется точное позиционирование пальца или ладони, для чего используются направляющие, на которые надо положить ладонь или палец. Это требует времени и не очень гигиенично. Достоинства – более высокая точность сканирования и стабильность биометрического признака (при внешнем воздействии) в сравнении со стандартными технологиями по отпечатку пальца.

Сканирование радужной оболочки и сетчатки глаза. Сканирование сетчатки не получило значительного распространения на рынке в отличие от более успешной в этом плане «радужки». Недостатки – большинство считывателей требует довольно точного позиционирования и, как следствие, процесс не самый быстрый. Устройства довольно дороги и не относятся к массовому сегменту рынка. Достоинства – одна из наиболее точных технологий с высокими характеристиками FAR и FRR. Высокая защищенность от подделки. Бесконтактная и гигиеничная технология.

Сканирование лица. Есть различные версии данной технологии (2D и 3D сканирование). Первый вариант в настоящее время довольно распространен и в некоторых вариациях используется, в том числе, в бытовых устройствах (смартфоны). Второй относится к верхнему ценовому и профессиональному сегменту рынка и недоступен для большинства потребителей в силу высокой стоимости. Недостатки – самые дешевые версии считывателей не очень хорошо защищены от подделки. Достоинства – степень защиты у авторитетных и солидных производителей обычно не хуже, чем у считывателей отпечатка пальца, стоимость таких устройств находится в среднем ценовом диапазоне, и они вполне доступны для потребителя. Это бесконтактная технология, следовательно, она удобна и гигиенична. Интерес рынка к данной технологии в настоящее время исключительно высокий.

Александр ГОРШКОВ:

– Практически во всех биометрических СКУД предлагается осуществлять идентификацию сотрудников по какому-то одному биометрическому признаку. Хотя программное обеспечение поддерживает два и более биометрических и небиометрических фактора. Например, идентификацию пользователя можно осуществлять на одних устройствах по отпечатку пальца, а на других – по рисунку вен ладони. Это очень удобно и позволяет оптимизировать затраты на закупку биометрического оборудования. Однако это решение не позволяет осуществить регистрацию сотрудника без его личного присутствия. Дополнительно требуется получение согласия сотрудников на хранение и обработку их персональных биометрических данных. Использование государственной централизованной системы учёта биометрических данных позволило бы исключить эту формальность.

Роман ГОРПИНЧЕНКО:

– К преимуществам биометрических СКУД следует, в первую очередь, отнести возможность идентификации и аутентификации пользователя по уникальным параметрам лица, отпечатка пальца, рисунка ладони, структуре сетчатки глаза. Такие данные в высшей степени сложно подделать, а мультифакторные схемы доступа, например, по рисунку лица и отпечатку пальца, позволяют свести к нулю риски. Пользователям не нужно использовать такие иден-

тификационные методы как пароли, карты доступа или радиометки, что радикально сокращает риск не авторизованного использования.

К недостаткам можно отнести сравнительно высокую стоимость таких устройств, а также наличие специфических требований к эксплуатации и обслуживанию.

Андрей ГАБЕЛКО:

– Одно из основных и очевидных преимуществ – контроль доступа не привязан к материальным носителям или информации, требующей запоминания (PIN-ы, коды, пароли), а связан с неотъемлемыми биометрическими характеристиками самого человека. То есть переход от принципов «я имею», «я знаю» к принципу «я есть». Это главное, так как существенно повышается надежность СКУД с точки зрения обеспечения безопасности.

Пропускная способность. Ряд биометрических технологий позволяют организовать биометрический СКУД с высокой пропускной способностью (до 60-80 человек/мин через точку прохода), недоступной традиционным СКУД.

Несомненным преимуществом является простота и удобство для конечного пользователя – «посмотрел – прошёл». Плюс, в ряде случаев снижаются операционные издержки поддержания СКУД, если принимать во внимание полную стоимость владения такой системой на горизонте в несколько лет.

К текущим, надеюсь, временным недостаткам можно отнести трудности сбора качественных биометрических шаблонов и относительное влияние на работу биометрических СКУД внешних условий при идентификации.

Еще можно отметить более высокую стоимость реализации биометрической СКУД по сравнению с традиционной. Но это, как «качели»: цена рисков / цена решения, и здесь каждый решает для себя сам, что ему важнее – сэкономить и, вероятно, иметь проблемы, или заплатить за обеспечение высокого уровня безопасности и надежности.

Денис СОКОЛОВ:

– Очевидное преимущество – это высокий уровень безопасности, так как биометрические признаки у каждого человека уникальны, их не передать и не подделать.

С точки зрения пользователя биометрия и удобнее, и неудобнее одновременно. Удобство в том, что палец или ладонь не забудешь дома, как карту или смартфон. Неудобство – обычно биометрическая идентификация занимает больше времени и требует больше действий от пользователя, чем, например, просто поднести карту куда-то в район считывателя, если мы не говорим об идентификации по лицу. Этот метод – самый удобный для пользователей, так как вообще ничего особого не требует от проходящего, но пока не самый надежный для предприятий с высокими требованиями к безопасности.

Андрей ХРУЛЕВ:

– Главным преимуществом использования биометрических СКУД является значительное повышение уровня безопасности охраняемых территорий и объектов. А также удобства получения допуска на охраняемую территорию. К примеру, больше нет необходимости носить с собой пропуск, так как пропуском могут являться отпечатки пальцев или даже собственное лицо, всё зависит от того, какая СКУД используется. Так же в зависимости от используемой на объекте системы, может происходить не только пропуск лиц, занесенных в базу, но и подсчет количества людей. Существует возможность выявления преступных элементов, если они занесены в систему, а соответственно снижение угрозы беспорядков и террористических актов.

ВОПРОС ДЛЯ ОБСУЖДЕНИЯ

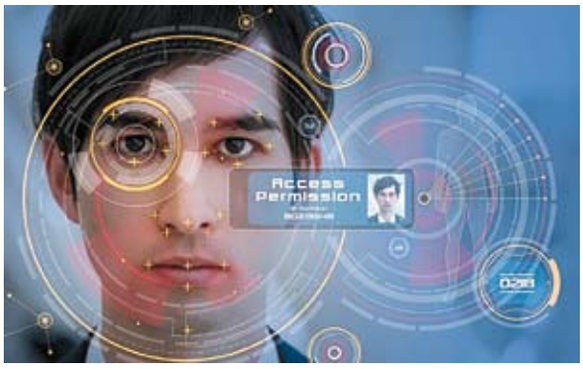
Какие факторы сдерживают применение и развитие биометрических СКУД?

Алексей ГИНЦЕ:

– Список таких факторов становится все меньше. Биометрические технологии получили «второе дыхание» на фоне их активного распространения в бытовой сфере, в IT и в банках. Биометрия долгое время была экзотикой из разряда «по улицам слона водили» и оставалась уделом узкого круга профессионалов и потребителей. После активного внедрения в сфере интернет-банкинга, распространения биометрических технологий в ноутбуках и смартфонах, она стала восприниматься потребителями как нечто привычное и перешла из разряда экзотики в область повседневности.

Александр ГОРШКОВ:

– Ни один руководитель не поддержит выделение дополнительных средств на замену или модернизацию того, что, по общему мнению, справляется с поставленными задачами. И только случай угрозы возникновения или выявления экономического ущерба, хищений или других угроз непрерывному функционированию производственных процессов, в том числе, полное прекращение деятельности организации из-за нарушения регламентирующих требований – может стать поводом для рассмотрения возможности модернизации СКУД.



Роман ГОРПИНЧЕНКО:

– Ключевой сдерживающий фактор - это цена оборудования и требования к навыкам инсталляторов и службы эксплуатации.

Андрей ГАБЕЛКО:

– В ряде случаев более высокая стоимость в сравнении с традиционными. Недостаточные знания конечных заказчиков и пользователей о возможностях и преимуществах биометрических технологий и биометрических СКУД. Инертность самих поставщиков СКУД. Подавляющее большинство из них работает по принципу «только под конкретный проект» и не готово приложить минимальные усилия на интеграцию с биометрией.

Денис СОКОЛОВ:

– Здесь можно выделить две основные причины: технологическую и социальную.

Технологическая состоит в том, что работа алгоритмов распознавания биометрических данных не идеальна, то есть существует вероятность возникновения ошибок.

Социальная причина состоит в нежелании некоторых сотрудников предоставлять свои биометрические данные для нужд СКУД.

Андрей ХРУЛЕВ:

– Сдерживающих факторов при применении и развитии биометрических СКУД не так уж и много, одним из них является относительно высокая стоимость таких систем. Но непрерывное развитие, эксперименты и совершенствование алгоритмов приводят к оптимизации необходимого оборудования, что напрямую влияет на финальную стоимость внедрения.

ВОПРОС ДЛЯ ОБСУЖДЕНИЯ

Как вы оцениваете развитие нормативно-технической базы? Есть ли необходимость изменить или дополнить законы, нормативные правовые акты?

Алексей ГИНЦЕ:

– Лучший закон – это жизнь. Она сама расставит все по местам. Совершенствовать законы надо, но не надо превращать этот процесс в буффонаду.

Александр ГОРШКОВ:

– Нормативная база неравномерно регулирует требования к обеспечению необходимого уровня контроля доступа для различных отраслей. Как это ни странно, мне лично пришлось столкнуться с позицией одного юриста, который аргументировал отклонение замечаний к нормативному документу с требованиями по организации управления доступом для телекоммуникационных компаний тем, что на это у них нет средств! И в то же время в других отраслях есть положительные примеры. Скажем, принято постановление правительства РФ №969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности».

Роман ГОРПИНЧЕНКО:

– Нет сомнения, такая необходимость есть. В Европейском союзе принята директива GDPR. В России есть соответствующие законодательные акты, которые регулируют обращение с персональными данными пользователей, по сути целевыми для биометрии. Это, в свою очередь, заставляет производителей создавать оборудование с учётом этих требований. Ведущие производители и наша компания, в том числе, этому уделяют серьёзное внимание и стараются работать на опережение, следя за развитием законодательных трендов в области защиты персональных данных. Развитие правовой базы, вместе с тем, часто сталкивается с дилеммой «Безопасность/Приватность», которую в разных странах решают по-своему, полагаясь на традиции права, а также исторически сложившиеся реалии.

Андрей ГАБЕЛКО:

– Что касается нормативных документов по биометрическим СКУД, то они ничем принципиальным не отличаются от «нормативки» для обычной СКУД. Другое дело, нормативная база по биометрии, действительно, пока не до конца совершенна. Но это не упрек в адрес биометрии. Просто эта область всё еще молодая, значительно моложе СКУД, и она постоянно развивается и совершенствуется (в отличие от просто СКУД, где принципиально нового давно уже нет). Биометрические технологии опережают развитие нормативно-правовой базы. Поэтому и могут возникать проблемы.

Денис СОКОЛОВ:

– Считаем, что законодательство предъявляет достаточные требования к регулированию сферы применения технических средств и в большинстве своем не создает больших препятствий для развития и модернизации технических средств обеспечения безопасности, в частности, СКУД.

Однако инновационные разработки появляются довольно быстро, поэтому в среднесрочной перспективе законодатель, как нам кажется, должен будет актуализировать нормы и требования, привести их в соответствие с уровнем технического прогресса.

Андрей ХРУЛЕВ:

– Наша биометрическая система распознавания лиц получила сертификат ФСБ о соответствии требованиям постановления правительства № 969 в 2018 году. Сегодня мы можем с полным на то основанием говорить о целесообразности/окупаемости сертификации.

Эффекты для бизнеса – это, прежде всего, обеспечение безопасности при полном соответствии требованиям законодательства, что нивелирует предписания, гарантирует соблюдение нормативных требований. Кроме того, к ключевым эффектам для бизнеса можно отнести опыт по созданию сложных систем безопасности.

ВОПРОС ДЛЯ ОБСУЖДЕНИЯ

Какие особенности в развитии СКУД вы хотели бы отметить?

Алексей ГИНЦЕ:

– Усиление требований заказчиков по защищенности отдельных устройств, каналов связи и системы в целом. Высокая востребованность интеграции СКУД не только с другими подсистемами безопасности, но и с CRM, HRM, ERP-системами, программами внутреннего документооборота, бухгалтерскими программами вроде «1С» или «БОСС-Кадровик». Огромное внимание потребителя к эффективности и потенциалу, заложенному в управляющее ПО, перечню имеющихся сервисов и возможностей управления, оперативного получения информации руководством предприятия.

Александр ГОРШКОВ:

– Текущая ситуация со СКУД напоминает «лихие 90-е», когда люди массово стали ставить железные двери в свои квартиры, офисы и дома. Это могли быть двери из стали толщиной в пять миллиметров, большие тяжелые многослойные, выдерживающие несколько очередей из автомата, которые устанавливались со скрытыми петлями, чтобы их невозможно было срезать. Ригельный замок блокировал дверь длинными стальными планками. Выломать такую дверь было практически невозможно. Но специалисты, зарабатывающие методом тихой экспроприации, улыбались и плакали от умиления. Вскрыть такую дверь для них не представляло проблем.

Пластиковые карты некогда современных систем контроля доступа уже давно не обеспечивают надлежащей безопасности. Они теряются, копируются и не позволяют однозначно сказать, кому был предоставлен доступ. Осознание этой уязвимости сделает неизбежным модернизацию классических СКУД, которая приведёт к отказу от использования карт доступа и переходу на многофакторную биометрическую идентификацию.

Роман ГОРПИНЧЕНКО:

– Развитие системы контроля доступа, в принципе, можно назвать скорее консервативным. Новым технологиям требуется достаточно много времени для широкого распространения в отрасли. Также необходимо отметить национальные аспекты развития систем в России и за рубежом, когда прогрессивные СКУД обходят нас стороной. Помимо этого, персональные данные пользователей, с которыми необходимо работать для внедрения биометрических систем, заставляет привлекать к решению задачи более широкий круг специалистов, а также иметь в виду ответственность за использование данных в информационных системах. Тем не менее, мы считаем, что эти особенности отразятся на динамике внедрения биометрических СКУД, но не изменят общего направления, имеющего, конечно, положительный тренд.

Андрей ГАБЕЛКО:

– Так как я являюсь не поставщиком или разработчиком СКУД, а разработчиком/поставщиком биометрии (хотя бы и для СКУД), то могу лишь «взглянуть со стороны». Отмечу положительное движение/интерес СКУД-овцев к более современным (чем пресловутый Wiegand) интерфейсам/протоколам взаимодействия, например, таким, как OSDP. Ну, и, конечно же, постепенный рост интереса к биометрическим СКУД.

комплекс инженерно-технических средств
охраны периметра, территорий,
акваторий и верхней полусферы
от БПЛА «Мурена-КС»

Umirs

БИОМЕТРИЧЕСКИЙ КОНТРОЛЛЕР ДОСТУПА

программно-аппаратный комплекс предназначен
для управления доступом в помещение

для подтверждения личности используется изображение лица

БЕЗОПАСНОСТЬ

вероятность ошибочного допуска
менее 0.0001%

АВТОНОМНОСТЬ

работа без выделенного сервера
и доступа в Internet

СИНХРОНИЗАЦИЯ

регистрация на одном контроллере
дает возможность прохода на любом другом

ВАНДАЛОСТОЙКОСТЬ

блок управления находится внутри
охраняемой зоны, может применяться
вандалостойкая IP-камера

ГИБКОСТЬ

работа в режиме шлюза, интеграция
в системы охраны серии «Мурена»

ЗАО «ЮМИРС», www.umirs.ru, Россия, г. Пенза, ул. Антонова, 3, тел./факс: +7 (8412) 69-84-01, manager@umirs.ru
Представительство в Москве, Россия, г. Москва, Сормовский пр., д. 5/1, оф. 208, тел./факс:(499) 722-66-01, (495) 740-48-14

Денис СОКОЛОВ:
– Наверное, здесь трудно быть оригинальным, так как рынок СКУД довольно консервативен, и тренды здесь развиваются не год и не два. Однако отметим, что важнейшей остается тенденция к сближению отрасли СКУД с IT-отраслью. То есть рынок, если говорить о технологических решениях, движется в сторону контроллеров-компьютеров с развернутыми на них Linux, тотальным шифрованием любого трафика, использование искусственного интеллекта и «облачных» систем, расширению интеграционных возможностей не только по отношению к другим системам безопасности, но и к информационным системам объектов.

Андрей ХРУЛЕВ:
– Современные интеллектуальные алгоритмы способны распознать лицо человека с высокой точностью, поэтому рынок биометрических систем считается одним из самых перспективных. Биометрические системы распознавания лиц уже доказали свою эффективность, и сегодня многие компании, независимо от размера и сферы деятельности, инициируют замену привычных СКУД на биометрические.

ВОПРОС ДЛЯ ОБСУЖДЕНИЯ
Каковы перспективы развития СКУД?

Алексей ГИНЦЕ:
– Одно из наиболее востребованных в перспективе и емких по объему направлений развития рынка систем безопасности.

Александр ГОРШКОВ:
– При выборе СКУД основными критериями является надёжность его работы и функциональные возможности. Например, автоматическая блокировка доступа сотрудника на всех объектах в момент оформления его увольнения. Со временем, большинство дополнительных возможностей будут поддерживаться многими разработчиками, и вопрос включения того или иного функционала будет определяться наличием закупленной лицензии. В этих конкурентных условиях на окончательный выбор решения станет влиять удобство использования. Постепенно карточные системы будут заменяться биометрическими, а биометрические решения будут развиваться в сторону «свободных рук», когда не требуются какие-то дополнительные действия, а идентификация осуществляется мгновенно во время прохода.

Роман ГОРПИНЧЕНКО:
– Несомненный тренд – это биометрические системы распознавания лиц на базе машин ИИ. Ведущие производители, в том числе, и наша компания, используют весь свой опыт для конструирования высокоэффективных автономных систем, находящих все большее применение в мире, уже не только как автономный контроллер СКУД, но и как терминалы учёта рабочего времени, с медиаинтерактивным контентом, биометрический считыватель для интеграции в существующую СКУД и ряд других применений. Такое оборудование станет еще более эффективным и доступным для пользователей в 2020-2021 годах.

Андрей ГАБЕЛКО:
– По моему убеждению, доля биометрических СКУД будет и дальше расти. Если сейчас я готов (субъективное ощущение) определить эту долю в 20% , то в перспективе 3-5 лет эта доля вполне может достигнуть 25-35%.

Денис СОКОЛОВ:
– Современные СКУД постепенно теряют некую «автономность» и двигаются к большей открытости – для того, чтобы максимально органично встраиваться в IT-инфраструктуру предприятий. Более того, СКУД уже берет и будет продолжать брать на себя все больше специфических возможностей, не только опосредованно связанных с контролем доступа (например, алкотестирование), но и с оптимизацией бизнес-процессов (упрощение кадрового учета, работа в составе ERP и так далее). Конечно, нельзя сказать, что эти тенденции характерны для всех производителей на рынке, но мы считаем, что именно в таком ключе должны развиваться современные системы контроля доступа.

Андрей ХРУЛЕВ:
– По данным агентства J'son & Partners доля биометрических СКУД в России к 2023 году составит 30%, демонстрируя среднегодовой рост не менее 15%. При этом доля СКУД с применением лицевой биометрии за последние годы выросла более чем на 10%, в то время как СКУД со сканерами отпечатков пальцев теряют популярность.

ВОПРОС ДЛЯ ОБСУЖДЕНИЯ
Ваше мнение о развитии биометрических технологий и их влиянии на СКУД.

Алексей ГИНЦЕ:
– Взрывной рост потребления и огромное влияние на рынок СКУД в целом. Биометрия будет все сильнее вытеснять классические технологии идентификации и захватит со временем львиную долю рынка.

Александр ГОРШКОВ:
– Практический опыт внедрения биометрической идентификации в СКУД подтверждает, что есть высокая вероятность наличия одного-двух сотрудников, у которых некоторые биометрические характеристики не могут быть идентифицированы. В результате предоставлять доступ таким сотрудникам приходится по традиционным идентификационным картам. Это не позволяет избавиться от недостатков и уязвимостей, присущих обычным системам контроля доступа. Надёжным решением в этом случае может стать мультимодальная биометрическая идентификация.

Роман ГОРПИНЧЕНКО:
– Фокусируясь на своих сильных сторонах и технологиях, лидеры рынка будут и впредь создавать качественные и эффективные оптические биометрические системы для решения широкого круга задач. В частности, миграция технологий искусственного интеллекта на конечные устройства позволила получить передовые модели, задающие новые стандарты в СКУД и в отрасли в целом. Следующим шагом мы видим ассимиляцию технологий контроля и управления доступом и видеонаблюдения.

Андрей ГАБЕЛКО:
– Большинство биометрических технологий постоянно развиваются и совершенствуются. Посмотрите, например, как «рвануло» за последние 3-4 года «лицо». Десятки команд, десятки решений (только ленивый не стал заниматься «лицом»). Появляются и другие альтернативные биометрические решения с еще более продвинутыми и надежными статистическими характеристиками, готовые «выстрелить» в самой ближайшей перспективе.
Еще важно отметить, что снижается стоимость биометрических решений. Всё это положительно влияет на рынок СКУД. Доля биометрии на рынке СКУД растет, сам рынок СКУД (в том числе, и благодаря биометрии) тоже растет.

Денис СОКОЛОВ:
– Уверены, что биометрические технологии будут усиливать свое влияние в СКУД по факторам, перечисленным в первом вопросе. Будут появляться все более совершенные алгоритмы, которые позволят уменьшить количество ошибок и время идентификации.

Редакция благодарит за помощь в подготовке «круглого стола» Василия Мамаева, заместителя директора НП РБО