Организация системы контроля доступа на предприятии

Евгений Шкляев, Марина Воскресенская

В статье рассмотрена организация системы контроля и управления доступом (СКУД). Даётся описание существующих видов СКУД, их составных частей, используемых технологий идентификации. Большое внимание уделено преимуществам и особенностям работы решений на базе СКУД BioSmart.

Введение

Система контроля и управления доступом на крупном промышленном предприятии является неотъемлемой частью эффективной работы организации. На крупных объектах работает огромное количество людей, приходящих к одному времени. При наличии КПП (контрольно-пропускного пункта) при одновременном приходе на работу сотрудников предприятия может образоваться очередь или столпотворение на входе. Если же КПП убрать, невозможно отследить время прихода и ухода сотрудников, присутствие их на рабочем месте, количество опозданий и прогулов.

Крупное предприятие может иметь несколько входов и выходов, а также большие распределённые территории, и привлекать к работе на каждом КПП сотрудника охраны бывает нерентабельно. А если на предприятии используется карточная система прохода и сотрудник забыл, потерял или испортил карту, регистрация в системе его прихода вручную может занять длительное время, что затрудняет проход на предприятие, а также появляется возможность ошибки, обусловленной человеческим фактором.

На предприятии может быть множество зданий различного назначения, например, отдельно стоящее производственное здание, отдельное административное и т.п., или в многоэтажном здании бывает необходимо разграничить доступ сотрудников в какие-либо помещения либо на каждый этаж. Организовать структуру доступа стандартными карточными системами бывает не так просто, и это занимает длительное время.

На территорию предприятия может заезжать и выезжать с неё через несколько ворот или шлагбаумов огромное количество автотранспорта. Когда транспортное средство подъезжает к КПП, охраннику необходимо вручную проверить уровень доступа транспортного средства, отметить в журнале посещений его въезд, а потом выезд.

Учёт рабочего времени является важным аспектом выплаты заработной платы сотрудникам. Человек может прийти и сразу уйти с рабочего места, договориться с охранником, чтобы он отметил ранний приход, а если на предприятии установлена карточная система контроля доступа, может передать свою карту коллеге и находиться в другом месте в рабочее время, в то время как работодатель будет думать, что сотрудник работает.

С этими проблемами сталкиваются многие руководители крупных предприятий и производств, не зная, что процесс можно автоматизировать, улучшить контроль посещаемости, убрать риски нахождения нетрезвых людей в ответственных цехах, автоматизировать учёт рабочего времени и оптимизировать расчёт заработной платы. Далее мы рассмотрим, как можно недорого, качественно и бесшовно решить все описанные проблемы, базируясь на современных системах видеонаблюдения и на инновационной системе контроля и учёта доступа (СКУД) BioSmart.

Решение по видеонаблюдению

Видеонаблюдение на предприятии стало неотъемлемой частью системы безопасности. Однако многие организации не устанавливают камеры, так как работают в условиях агрессивных сред: улица, горячие цеха, приморские территории, загрязнённые производства. Эту проблему решают современные защи-

Рис. 1. Серия камер GeoVision с высоким разрешением съёмки

Рис. 2. Камера серии GeoVision GV-LPR

щающие от агрессивных средств устройства – кожухи. Они могут быть с водяным охлаждением, позволяющим устанавливать устройства в условиях экстремально высоких температур (до +400°С), с обогревателем и вентилятором (обеспечивающими нормальную эксплуатацию устройства на улице при температуре от –50 до +70°С), с дворником, который будет протирать стекло (в условиях загрязнённых сред, например на предприятиях по добыче полезных ископаемых и т.п.), защищённые от соляных воздействий (приморские территории).

При установке на предприятии аналоговых камер видеонаблюдения руководители часто недовольны качеством съёмки, так как с имеющимся у аналоговых устройств разрешением сложно рассмотреть нештатные ситуации. Современные системы активно развиваются, технологический прогресс не стоит на месте. Производители улучшают качество устройств при снижении их стоимости. Новейшие IP-камеры GeoVision с высоким разрешением съёмки от 4 Мпиксел (2560×1440) до 12 Мпиксел (4000×3000) становятся всё более популярными (рис. 1). При этом, если раньше потребителей пугал объём хранения данных, в данный момент производители систем видеонаблюдения решили вопрос технологичным кодеком сжатия H.265, уменьшающим объём хранения данных на 30–40%, обладающим возможностью записывать происходящее только при движении в кадре, устанавливать так называемые зоны интереса ROI (Region of Interest), где важно вести качественную съёмку, а остальные участки будут записаны либо с меньшей скоростью (1–5 кадров в секунду), либо с ухудшенным разрешением. Комбинация всех этих возможностей позволяет вести высококачественную съёмку при сохранении глубины архива. Разрешение съёмки в 12 Мпиксел важно при распознавании лиц и идентификации объектов. При необходимости можно будет детально рассмотреть, кто именно совершил правонарушение.

На многих предприятиях установлены шлагбаумы или ворота при въезде на территорию организации. Охранник в ручном режиме открывает и закрывает шлагбаум или ворота для въезда и выезда транспортных средств, при этом учёт времени нахождения транспорта на территории, время заезда и выезда производится не всегда. Данный процесс легко автоматизировать благодаря установке всего двух камер уличного исполнения на каждый въезд и выезд с территории и программного обеспечения Revisor для распознавания автомобильного номера. Камера должна быть установлена в специализированный кожух, защищённый от попадания воды, а также снабжённый обогревателем для работы в зимнее время года. Разрешение съёмки камеры может быть минимальным – программному обеспечению Revisor достаточно разрешения 720 пиксел (1280×720) для безошибочного определения автомобильного номера. Главное условие – широкий динамический диапазон (WDR), для чёткого распознавания в ночное время с включёнными фарами. Для данных задач компания GeoVision разработала специализированную серию камер LPR (License Plate Recognition – распознавание автомобильных номеров). Серия камер (рис. 2) обладает высокой светочувствительностью, встроенной ИК-подсветкой и, главное, устраняет засветку от фар. В программное обеспечение Revisor заносится база автомобильных номеров, въезд которых на территорию предприятия разрешён (рис. 3). Когда транспортное средство подъезжает к шлагбауму, камера считывает государственный номер, а программное обеспечение сравнивает его с текущей базой (рис. 4). Если номер занесён в базу, ПО передаёт сигнал на контроллер и шлагбаум или ворота автоматически открываются. Если номер распознать не удалось, подаётся сигнал оператору системы, который принимает решение о пропуске автотранспорта в ручном режиме. Также может быть создана база времени въезда и выезда конкретных транспортных средств, есть возможность по государственному номеру найти время въезда или выезда ТС, автоматически считать время присутствия транспортного средства на территории предприятия, создавать базу гостевых номеров.

Организация СКУД на предприятии на основе оборудования Biosmart

Большинство организаций сталкиваются с рядом проблем в области безопасности и эффективного контроля доступа на свою территорию. В целях защиты объекта используются системы контроля и управления доступом (СКУД, или PACS – Physical Access Control System). СКУД – это совокупность программно-аппаратных технических

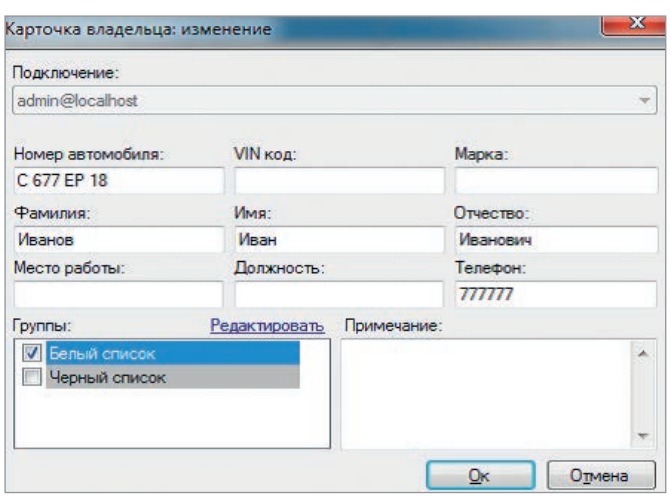


Рис. 3. Занесение государственных автомобильных номеров в базу Revisor

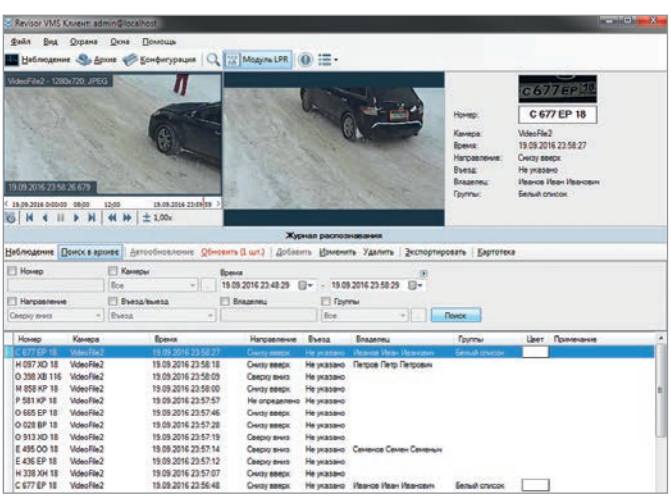


Рис. 4. Распознавание номера в ПО Revisor

средств безопасности, разграничивающая права прохода в помещения (зоны, территории) определённых категорий лиц и ограничивающая доступ лиц, не обладающих такими правами [1–5].

В настоящее время СКУД представляет собой сложный многоуровневый и многоцелевой автоматизированный комплекс организационных и технических мероприятий, для работы которого используются современные технологии, в том числе биометрическая идентификация, новейшее программное обеспечение и т.д. Такие системы контроля доступа позволяют обеспечить безопасность посетителей и объекта, могут решать задачи организации учёта рабочего времени и обеспечения сохранности материальных ценностей, упорядочивать передвижение людей по объекту, а также выполнять достаточно много других функций защиты и контроля. При этом с расширением функциональности растёт сложность и стоимость внедрения и обслуживания таких систем.

В общем случае СКУД подразделяются на сетевые, автономные и комбинированные.

Сетевые СКУД используются на больших объектах, так как эти системы способны управлять десятками пунктов прохода, используя для обмена информацией с пропускными конструкциями центральный пульт. Таким образом, сетевые системы могут управляться одним оператором, который имеет возможность осуществлять дистанционное и оперативное управление системными устройствами. Сетевые СКУД требуют достаточно развитой программной и аппаратной инфраструктуры, в частности, устройств сопряжения с компьютером, прокладки кабелей и витых пар и т.д. Такие системы довольно дороги при внедрении и в эксплуатации.

Автономные СКУД гораздо дешевле, а для небольших предприятий и компаний по эффективности сравнимы с сетевыми СКУД. Тем не менее, они имеют свои недостатки: дистанционно управлять ими нельзя, они не предназначены для управления многими пунктами пропуска, невозможно выполнять дополнительные функции по передаче информации о событиях.

Обычно на практике используют **комбинированные** системы, включающие функции как автономных, так и сетевых СКУД. Модульный принцип построения позволяет конструировать и наращивать СКУД в зависимости от текущих потребностей. Интегрированность систем (то есть возможность обеспечения их взаимодействия с различными системами охраны и обеспечения безопасности здания) позволяет реализовать работу сети исполнительных устройств СКУД с использованием универсальных интерфейсов.

Тем не менее, наиболее важным вопросом для СКУД является вопрос контроля доступа на объект и обеспечения идентификации субъекта. Среди использующихся в настоящее время способов идентификации одним из наиболее эффективных является биометрический способ, который нашёл широкое применение в организациях, где требуется повышенный уровень безопасности.

В биометрических системах идентификации распознаются не физические носители информации, а признаки или особенности самого человека, то есть уникальные характеристики, поэтому системы доступа и защиты информации, использующие биометрию, яв-

ляются не только самыми надёжными, но и самыми удобными для пользователей на сегодняшний день.

Методы биометрической идентификации подразделяются на статические и динамические. При этом статические методы используют в качестве базы для распознавания и идентификации объекта физиологические характеристики человека, например, папиллярные узоры отпечатков пальцев, скан сетчатки глаза, фрагменты генетического кода и т.п. Динамические методы строятся на поведенческих характеристиках человека – особенностях его подсознательных движений в процессе выполнения обычных действий (динамика клавиатурного набора, речевые модуляции и т.д.).

Рассмотрим эти методы немного подробнее.

Распознавание дактилоскопических признаков является одним из наиболее распространённых биометрических идентификационных методов при использовании в СКУД. При этом стоит заметить, что современные дактилоскопические считыватели не хранят сами отпечатки пальцев, а только некую их математическую модель, по которой отпечаток не восстанавливается.

По надёжности и скорости идентификации с дактилоскопическим методом сопоставимы методы лицевой термографии (идентификация по схеме расположения кровеносных сосудов лица) и методы распознавания по рисунку вен на руке. Инфракрасная камера сканирует фиксированные зоны на лице или руке, и термограмма, полученная в результате сканирования, является основой для идентификации человека как его уникальная характеристика. Этот метод позволяет распознавать человека, невзирая на температуру его тела или на процесс жизненного старения, а также после пластических операций или использования специальных масок, поскольку термограмма – это схема расположения внутренних кровеносных сосудов, и этот рисунок является абсолютно уникальным для человека.

Идентификация человека по форме кисти руки не является достаточно надёжным способом, поскольку в течение жизни и даже в достаточно короткие промежутки времени форма кисти может значительно измениться, что весьма усложняет идентификацию. К аппаратным недостаткам этого метода относятся сравнительно большие размеры устройства для сканирования – оно должно быть не менее размера кисти в плоскости, а в высоту должно составлять более 20 сантиметров. Достоинством этого метода является очень небольшой объём результата сканирования – математический «портрет» кисти руки составляет всего лишь 9 кбайт.

Достаточно надёжен биометрический метод идентификации по радужной оболочке и сетчатке глаза. Устройство сканирования в этом случае представляет собой высококачественную камеру, позволяющую сканировать сетчатку глаза с помощью инфракрасных лучей низкой интенсивности. Луч проходит через зрачок к кровеносным сосудам на задней стенке глаза, сканируя радужную оболочку, «отражающуюся» на задней части глаза. Тем не менее, у него есть довольно большие недостатки: во-первых, это дороговизна метода, а во-вторых, сетчатка глаза и радужная оболочка весьма подвержены изменениям даже при таких обычных явлениях человеческой жизни, как бессонница или повышенная нагруз-

ка на глаза, не говоря уже о том, что с возрастом расположение пятен на радужной оболочке глаз может измениться или человек может страдать такими заболеваниями, как глаукома или катаракта.

Наиболее достоверным методом идентификации является идентификация по фрагментам генетического кода человека. К сожалению, этот метод малопригоден в настоящее время для практического массового использования, поскольку он очень сложный, дорогостоящий и его технология недостаточно разработана для применения в режиме реального времени. В связи с этим метод идентификации по генетическому коду используется в основном в криминалистике, а также в исторических или палеонтологических целях.

Виды идентификации по характеристике голоса и по подписи относятся к динамическим методам биометрической идентификации. В настоящее время они применяются достаточно часто, но не являются настолько надёжными, как основные статистические методы. Так, идентификация по голосу используется обычно для контроля доступа к информации путём произнесения парольной фразы. Это достаточно удобно и просто. Но голос человека – довольно зыбкая характеристика, поскольку модуляции голоса одного и того же субъекта могут меняться в зависимости от настроения, состояния здоровья, возраста и множества других факторов. Дополнительной проблемой является шумовой компонент, который достаточно сложно отделить от общего голосового сигнала. Поэтому идентификация по голосу в настоящий момент применяется на практике относительно редко, особенно на крупных предприятиях с большим количеством сотрудников и посетителей.

Идентификация человека по его подписи на данный момент также недостаточно разработана для массового применения. Для использования этого метода должны применяться определённые устройства (специальные ручки или чувствительные к давлению столы, или то и другое в совокупности). При этом такой метод весьма долог и затратен, а процедуры распознавания неудобны в применении и достаточно громоздки. В связи с этим метод определения по подписи практически не применяется, за исключением особых единичных случаев.

Биометрические сканеры всё ещё дороги, хотя в последнее время их цена снизилась, поскольку в связи со всё большей востребованностью ведётся работа по их усовершенствованию, в том числе и в ценовом плане. Дополнительными недостатками являются невозможность применения биометрических считывателей на улице и сравнительно долгое время идентификации, что на практике выражается в задержках при необходимости контроля большого потока людей.

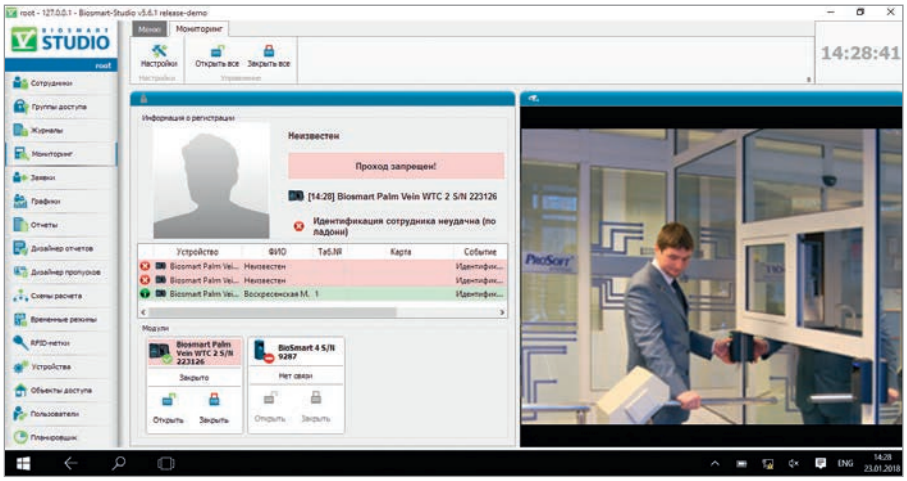


Рис. 5. Пример интеграции СКУД с видеонаблюдением

Тем не менее, именно точность биометрических методов идентификации является наиболее востребованным параметром при защите объектов и информации, особенно в последнее время, когда становится более важным снижение критического уровня уязвимости безопасности.

В связи с этим биометрические системы идентификации BioSmart становятся всё более конкурентоспособными на рынке систем СКУД. Системы идентификации на основе оборудования BioSmart оснащены как биометрическими считывателями (сканеры отпечатков пальцев или венозного рисунка ладони), так и считывателями карт RFID, что позволяет использовать разнообразные комбинации методов идентификации.

В настоящее время одной из самых распространённых биометрических СКУД отечественного производства является СКУД BioSmart.

СКУД на основе оборудования BioSmart представляет собой модульную сетевую распределённую систему, способную к интеграции с оборудованием других производителей (рис. 5). Эта система обладает возможностью разграничения прав доступа пользователей и управляется с центрального компьютера или сервера, к которому подключаются сканеры (как биометрические, так и считыватели RFID-карт, установленные в точках прохода).

Для работы с внешними датчиками на блоке управления реле предусмотрены два дискретных входа. Первый дискретный вход применяется для подключения выносной кнопки выхода из помещения. Второй дискретный вход может использоваться для подключения датчика открытия двери, датчика турникета, пожарной сигнализации. Все события по внешним датчикам фиксируются в журнале событий.

Для интеграции с устройствами сторонних производителей на плате контроллера BioSmart присутствуют вход и выход интерфейса Wiegand, работающего в диапазоне от 26 до 40 бит.

Выход интерфейса Wiegand позволяет интегрировать контроллер BioSmart в любую СКУД. В случае успешной идентификации контроллер Biosmart передаёт код карты на контроллер сторонней СКУД. В свою очередь, контроллер СКУД принимает решение о допуске и подаёт сигнал на исполнительное устройство (рис. 6).

Биометрические данные посетителей и пользователей регистрируются в программном обеспечении BioSmart-Studio. Для каждого пользователя можно в целях идентификации зарегистрировать отпечатки пальцев, рисунок вен ладони и код RFID-карты, присвоить право доступа в определённые точки. База данных содержит лишь математические шаблоны биометрических данных, что делает невозможным воссоздание графического изображения биометрических параметров. Это позволяет снизить возможность неконтролируемого доступа в результате возможных мошеннических действий по подделке оригинальных биометрических параметров.

Для идентификации пользователя предполагается простой алгоритм: поль-

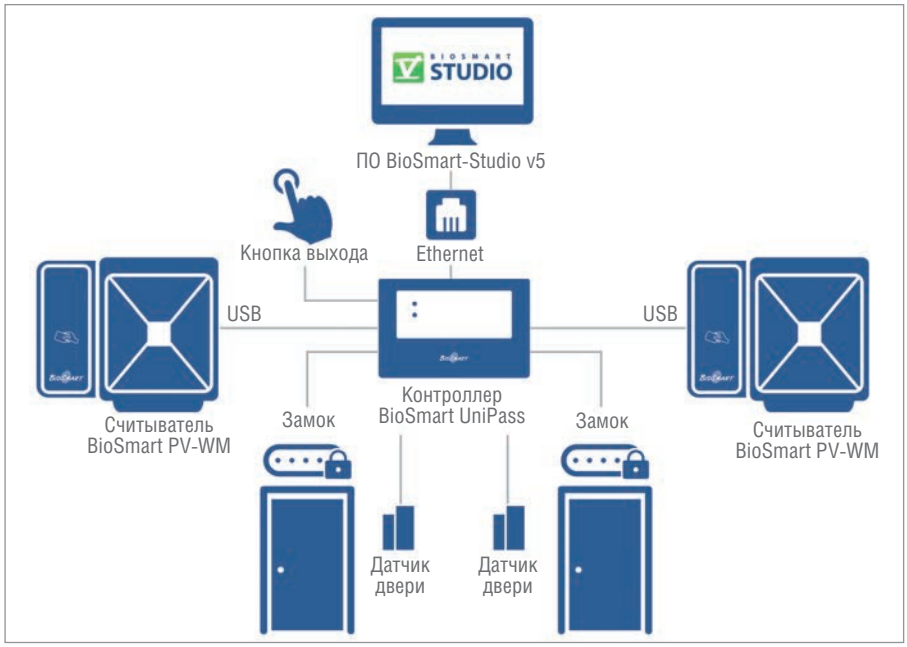


Рис. 6. Контроль доступа на базе UNIPASS

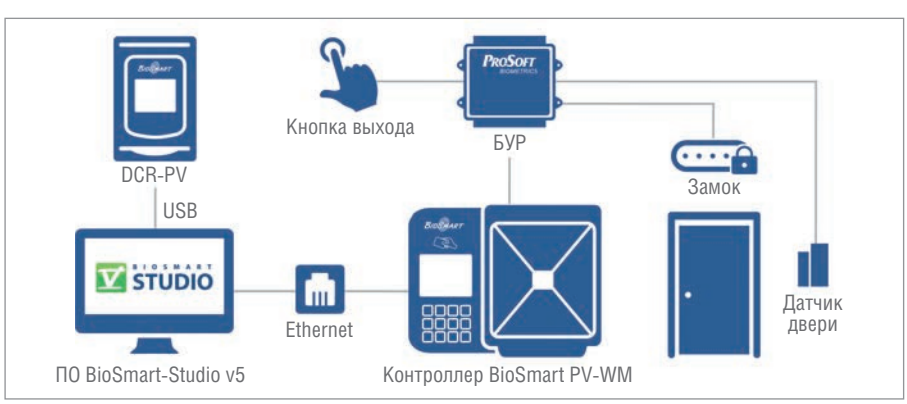
зователь прикладывает палец, ладонь или RFID-карту к сканеру, информация о пользователе передаётся на контроллер по локальной сети, в контроллере производится идентификация пользователя путём сравнения полученной информации с шаблоном биометрии либо с кодом RFID-карты, после чего осуществляется доступ.

Обычно на крупных предприятиях или объектах с большой базой данных работников и посетителей необходимо применение серверной идентификации. В этом случае идентификация пользователей осуществляется на внешнем сервере, что позволяет значительно повысить скорость идентификации и доступа благодаря использованию вычислительных мощностей внешнего сервера. Так, в этом случае в среднем скорость идентификации 10 тысяч отпечатков на сервере не превышает одной секунды.

Для режимных предприятий возможна организация доступа только по карте либо по комбинации RFID-карта + отпечаток пальца или ладони. При этом обязательно применение магистралей Ethernet и контроллеров Biosmart в исполнении со встроенным портом Ethernet (рис. 7).

Объём базы данных отпечатков в СКУД BioSmart возможно увеличить на порядки при использовании карт с внутренней памятью (например, карт формата Mifare). В этом случае биометрические параметры пользователя записываются в память карты, и человек становится носителем собственного шаблона. Идентификация при этом происходит следующим образом. Пользователь прикладывает карту к сканеру контроллера, передавая в его память шаблон отпечатка, после чего прикладывает свой палец к сканеру. Контроллер сравнивает шаблон с приложенным отпечатком, производит идентификацию и осуществляет доступ.

Таким образом, в зависимости от требуемой функциональности СКУД на основе оборудования BioSmart позволяет реализовать алгоритмы любой сложности минимальными средствами, а также снизить расходы на преобразование карточной системы в биометрическую. При этом достаточно заменить сканеры, поскольку контроллер, база данных сотрудников, исполнительные устройства и кабельные трассы остаются прежними.



Условные обозначения: DCR-PV – считыватель рисунка вен ладони; БУР – блок управления реле.

Рис. 7. Контроль доступа на базе PV-WTC

Заключение

Благодаря современным биометрическим устройствам распознавания можно минимизировать присутствие нежелательных лиц на территории предприятия, оптимизировать время прохождения сотрудников через КПП, ограничить доступ в необходимые помещения, автоматизировать доступ автотранспорта на территорию предприятия. При этом сотрудник не должен носить с собой дополнительные устройства, которые он может потерять, сломать или передать другому человеку. Система контроля и учёта доступа BioSmart в комбинации с системой видеонаблюдения является оптимальным решением для безопасности предприятий. ●

Литература

1. Яковлев Е.А. Биометрические технологии и системы контроля в управлении // Экономика и управление в XXI веке: тенденции развития : сб. материалов XXXVI Межд. научно-практ. конф., 2017.
2. Максимов Р.Л., Рафиков А.Г. Разработка автоматической СКУД повышенной безопасности на базе типового решения СКУД Biosmart с использованием автоматного подхода // Вопросы кибербезопасности. – 2015. – № 5 (13).
3. Смолин М.Ю., Борисов А.П. К вопросу об использовании систем биометрической защиты при обучении студентов // Современные технологии в мировом научном пространстве : сб. статей Межд. научно-практ. конф., 2017.
4. Денисьев С.А. Биометрия в УИС // Актуальные проблемы деятельности подразделений УИС : сб. материалов Всероссийской научно-практ. конф. – ФКОУ ВПО «Воронежский институт ФСИН России», 2012.
5. Арсениев А.Н., Балаев А.К., Макаренко Ю.А. Методы биометрической идентификации: потенциал применения в системах контроля и управления доступом // Новая наука: проблемы и перспективы. – 2016. – № 121-3.

Авторы – сотрудники фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru