Крахмалев Александр Кузьмич, начальник отдела ФГУ НИЦ «Охрана» МВД России, полковник милиции, к.т.н.

Оборудование систем контроля доступа для объектов особой важности и повышенной опасности

Обеспечение безопасности **объектов особой важности,** повышенной опасности и жизнеобеспечения (критически важных объектов — **КВО**) на фоне роста **террористических угроз** является сегодня весьма актуальной проблемой. Захват, вывод из строя или нарушение функционирования таких объектов и перевозимых специальных грузов чреваты крайне негативными последствиями и могут нанести крупный или невосполнимый ущерб государству и обществу.

К таким объектам могут относиться:

- объекты высших органов власти, правительственные учреждения, крупные объекты кредитно-финансовой сферы;
- объекты особо важного административного, общественного и промышленного значения с высокими требованиями к системам жизнеобеспечения и безопасности;
- объекты топливно-энергетического комплекса, ядерноопасные, радиационно, химически и биологически опасные объекты, электростанции, в том числе атомные, **гидротехнические сооружения,** тоннели, мосты, газонефтепроводы, склады горюче-смазочных материалов и т.п.;
- объекты микробиологической и фармацевтической промышленности, объекты по переработке и хранению наркотических веществ, сильнодействующих ядов и химикатов, психотропных веществ и препаратов;
- объекты, являющиеся архитектурными памятниками, музеи, здания для хранения архивов, художественных и других подобного рода культурных и материальных ценностей, объекты культа;
- объекты (территории) жизнеобеспечения;
- метрополитен, подземные сооружения особо важного значения;
- жилые многоэтажные дома;
- объекты массового пребывания людей: школы и больницы, кинотеатры, стадионы, вокзалы, аэропорты и т. д.;
- **специальные грузы,** перевозимые автомобильным, железнодорожным транспортом, судами речного и морского флота.

Обеспечение безопасности подобных объектов требует **комплекса мер,** направленных на предупреждение, пресечение и устранение угрозы или опасной ситуации. **Комплекс мер** должен основываться на принципах **системного подхода** к деятельности по обеспечению безопасности, как на этапах организации, подготовки, проектирования, так и в процессе эксплуатации, и включать в себя совокупность **организационных и технических** мероприятий, то есть **систему комплексной безопасности.**

Не умаляя значения организационно-правовых и профилактических методов борьбы с терроризмом, следует отметить, что их практическая реализация невозможна без современных **технических средств.** Номенклатура таких средств достаточно широка и позволяет при грамотном проведении единой технической политики, умелом сочетании и применении технических средств обеспечить надежную защиту любого объекта, обнаружить и нейтрализовать террористические угрозы практически в любых условиях и при любых сценариях их развития. Поэтому во всем мире наблюдается **устойчивая тенденция к расширению сферы задач безопасности, возлагаемых на технические средства.**

Результаты изучения перспектив развития как отечественных, так и зарубежных средств безопасности позволяют утверждать, что для обеспечения безопасности КВО наилучшим образом подходят **интегрированные системы безопасности (ИСБ),** которые представляют собой объединение на единой программно-аппаратной основе систем охранно-пожарной сигнализации (ОПС), систем охранного телевидения (СОТ) и систем контроля и управления доступом (СКУД). ИСБ предназначены для решения вопросов обеспечения безопасности крупных и средних объектов, объектов особой важности и повышенной опасности, объектов кредитно-финансовой сферы и позволяют решать на новом качественном уровне задачи по обеспечению безопасности объектов.

ФГУ НИЦ «Охрана» совместно с ведущими отечественными предприятиями, работающими в этом направлении, были разработаны и внедрены в серийное производство интегрированные системы: «Рубеж», «Аккорд-512», «Орион», «Кодос-А20».

Эти современные ИСБ обеспечивают:

- модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты;
- контроль и управление доступом через точки входа (двери, турникеты, шлюзы, шлагбаумы);

- видеонаблюдение, видеоконтроль и видеорегистрацию тревожных ситуаций;
- управление установками пожарной автоматики;
- управление инженерными системами здания (кондиционирования, отопления, вентиляции, оповещения, аварийной сигнализации);
- защищенный протокол обмена по каналам связи, имитостойкие шлейфы сигнализации;
- возможность использования для взятия под охрану/снятия с охраны дистанционных радиокарт и электронных ключей;
- речевое предупреждение дежурного о тревожных событиях, возможность записи и воспроизведения речевых сообщений;
- отображение состояний зон, разделов, точек доступа, приемно-контрольных приборов, считывающих устройств, видеокамер на графических планах помещений с подробными текстовыми пояснениями;
- разграничение полномочий дежурных, операторов, администраторов за счет многоуровневой системы паролей и возможность подключения биометрических систем ограничения доступа к программам АРМ;
- протоколирование всех событий, происходящих в системе;
- развитую диагностику работоспособности всех блоков и устройств системы;
- удаленную передачу данных и защиту информации по различным каналам (выделенным проводным, телефонным через модемы, оптоволоконным, радиоканалам, каналам сотовой связи, цифровым сетям ISDN).

Кроме этого, ИСБ позволяют оптимальным образом сократить людские и материальные ресурсы, а также финансовые затраты (в том числе бюджетные) на оборудование объектов, эксплуатацию аппаратуры и содержание охранников.

Неотъемлемой частью **ИСБ,** в особенности применительно к решению задачи защиты **КВО,** служат **системы контроля и управления доступом.**

СКУД играют особую роль в системах безопасности, так как контроль доступа является фундаментальным понятием процесса обеспечения безопасности. Любая система безопасности должна определить человека по принципу «свой/чужой» для защиты объекта от проникновения посторонних лиц или для защиты человека от опасных факторов воздействия, если они имеются на объекте.

СКУД — самое интенсивно развивающееся направление в технике обеспечения безопасности. Это связано с целым рядом факторов.

Во-первых, СКУД могут обеспечить полную автоматизацию контроля и управления доступом, что в общем случае приводит к экономии средств, выделяемых на обеспечение безопасности.

Во-вторых, СКУД могут решать такие задачи, как учет рабочего времени, быстрое определение местонахождения сотрудника, управление лифтами, освещением, вентиляцией и т. д.

В-третьих, СКУД позволяет решить вопрос повышения безопасности на объекте в течение всего времени суток, так как она обеспечивает эффективный контроль над помещениями, сотрудниками и посетителями, в то время как системы охранной сигнализации функционируют, как правило, только в нерабочее время. Кроме того, СКУД позволяет сотрудникам, обладающим необходимыми полномочиями, чувствовать себя свободно и иметь возможность перемещаться по зданию или территории объекта без помех.

Автоматизация процесса доступа человека на объект или доступа человека к информации (управлению информационными системами и ресурсами) позволяет также снизить «человеческий» фактор, который в системах безопасности имеет негативный характер.

Широкое распространение автоматизированных многофункциональных СКУД до недавнего времени сдерживалось во многом их довольно высокой стоимостью, так как реализация необходимой номенклатуры требований объясняется значительной сложностью создания и внедрения автоматических систем, полностью заменяющих человека в процессе контроля доступа. Несмотря на кажущееся однообразие выполняемых операций, на самом деле анализируется большой объем самой разнообразной информации и при возникновении любых, даже нетиповых ситуаций всегда требуется принять конкретные решения. Понятно, что реализация соответствующих задач требует применения многофункциональных, технически совершенных автоматических устройств и систем, имеющих весьма высокую стоимость.

Однако в настоящее время эти системы активно развиваются и в них появляются новые технологии.

В основе работы СКУД заложен принцип сравнения тех или иных **идентификационных признаков,** принадлежащих конкретному физическому лицу или объекту, с информацией, заложенной в памяти системы. Поэтому прогресс в области СКУД связан, прежде всего, с развитием новых технологий **идентификации.**

Среди наиболее перспективных и развивающихся технологий идентификации можно отметить **радиочастотную и биометрическую.**

Системы **радиочастотной идентификации** и регистрации объектов **RFID** (Radio Frequency IDentification) получили широкое распространение с начала 90-х годов. В системах контроля доступа стали использоваться дистанционные пластиковые карты, которые получили название Proximity. По сравнению с уже существовавшими картами со штриховым кодированием, магнитными картами, картами Виганда и др., дистанционные

карты технологии RFID обладают рядом существенных преимуществ. Идентификация производится по уникальному цифровому коду, излучаемому расположенной в карте специализированной микросхемой — транспондером **(transmitter/responder:** передатчик — приемник). Внутри карты расположена также антенна, соединенная с микросхемой транспондера.

Код принимается с помощью приемо-передающего устройства — считывателя. Считыватель содержит в своем составе передатчик и антенну, посредством которой излучается электромагнитное поле определенной частоты. Попавшие в зону действия считывателя карты активизируются, получают за счет индуктивной связи энергию для питания и передают на считыватель цифровой код, записанный в памяти микросхемы.

Прогресс в области современных радиочастотных идентификаторов связан с освоением новых частотных диапазонов (8,2 МГц, 13,56 МГц, 850–950 МГц и 2,4–5 ГГц). Более высокие частоты обеспечивают меньшие габариты антенны и большую дальность считывания, а также быстрый обмен данными, поэтому возможно на базе транспондеров обеспечить двухсторонний обмен данными между идентификатором и считывателем с возможностью кодирования и защиты информации. Более высокие частоты позволяют также обеспечить идентификацию быстродвижущихся объектов — транспортных средств.

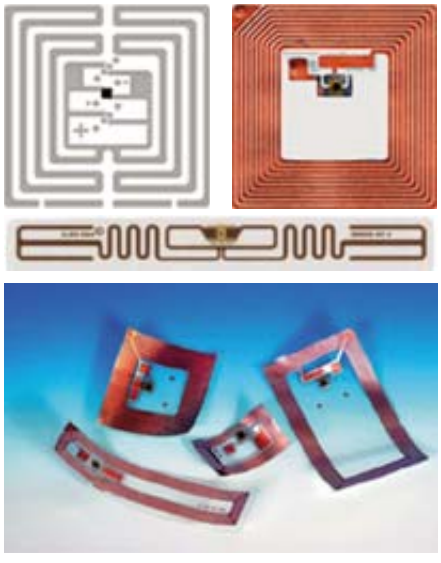


Рис. 1.
Идентификаторы RFID в виде тонкопленочных меток

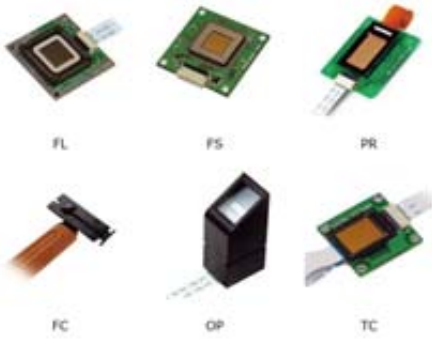


Рис. 2.
Дактилоскопические сканеры различных технологий

Высокая частота позволяет выполнять антенну в печатном или интегрированном виде, что обеспечивает производство дешёвых и малогабаритных идентификаторов. Такие характеристики, в свою очередь, могут обеспечить защиту идентификаторов доступа от несанкционированного использования и копирования, а также обеспечить скрытую установку для контроля перемещения предметов и грузов. На рисунке 1 приведен пример конструктивного исполнения RFID меток.

Наибольший интерес в области развития идентификации в СКУД проявляется к биометрической технологии. Применение биометрических технологий в составе этих систем позволит существенно поднять уровень безопасности объектов, а также решить задачу защиты самих систем от несанкционированного вмешательства и доступа.

Среди биометрических технологий наиболее широко применяются методы идентификации по отпечаткам пальцев. Прогресс в этой области связан с успехами в математическом обеспечении методов распознавания, которые позволили создать надежные программные продукты, а также в развитии устройств считывания — дактилоскопических сканеров. На смену традиционным оптическим сканерам приходят новые технологии, такие сканеры, как: термо, емкостные, пьезо, ультразвуковые и др. Они обладают меньшей стоимостью, более высокой надежностью, меньшими габаритами, более высокой защищенностью от имитации.

На рисунке 2 приведены различные модели дактилоскопических сканеров — считывателей отпечатков пальцев.

Появление подобных новых технологий приводит к снижению стоимости биометрических систем при сохранении высоких показателей надежности, что делает их доступными для применения на самых различных объектах — от электронных дверных замков до объектов с высокой степенью защищенности доступа.

На базе приведенных выше моделей сканеров в ФГУ НИЦ «Охрана» совместно с предприятиями-изготовителями были разработаны биометрические считыватели для применения в

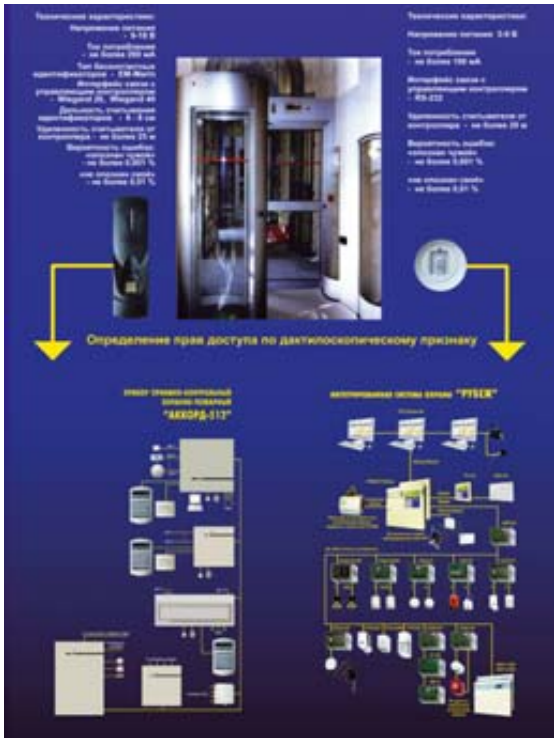


Рис. 3.
Биометрические считыватели в составе ИСБ

составе интегрированных систем «Рубеж» и «Аккорд-512» (рисунок 3). Считыватели имеют несколько вариантов исполнения для различных случаев применения: в составе соответствующих интегрированных систем; с универсальным интерфейсом для применения в ИСБ и СКУД других производителей; в исполнении для автономных СКУД.

Ниже приведены краткие характеристики биометрических устройств.

1. Шифроустройство для систем контроля и управления доступом ШУ024-2 ЯЛКГ.425723.003 ТУ

Прибор является устройством считывания дактилоскопической информации пользователя по отпечатку пальца, с возможностью управления и контроля прохода на охраняемую территорию, и предназначен для построения системы контроля доступа.

Основные возможности:

- Считывание дактилоскопической информации по отпечатку пальца человека.
- Конфиденциальность внешних биометрических данных.
- Закрепление за пользователем уникального идентификатора.
- Приём идентификатора от УСК по Wiegand26.
- Передача идентификатора к СКУД по Wiegand26.
- Идентификация пользователя по отпечатку пальца.
- Идентификация пользователя по двум признакам.
- Автономный режим работы.
- Режим работы в составе СКУД.
- Управление электромеханическим замком двери.
- Энергонезависимое хранение идентификаторов.
- Администрирование БД идентификаторов пользователей.
- Конфигурирование функциональности по RS-232.
- Световая и звуковая индикация событий.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ	
Основная идентификация пользователя, тип	**Биометрическая идентификация по отпечатку пальца человека**
Сканер отпечатка пальца человека, тип	тепловой
Ёмкость БД пользователей, кол-во идентификаторов	9000
Время верификации пользователя, не более, С	1
Уровень EER (Equal Error Rates — точка, в которой вероятность ошибки первого рода равна вероятности ошибки второго рода)	<0.1 %
Напряжение внешнего источника питания постоянного тока, В	10,5 … 28
Ток, потребляемый прибором в дежурном режиме при отключенных внешних потребителях (дополнительном УСК, электромагнита дверного замка, кнопки выхода) от источника питания 12 В, не более, А	0.4
Интерфейс для подключения дополнительного УСК	Wiegand26
Интерфейс для подключения к СКУД	Wiegand26
Напряжение коммутации контактов электромагнитного реле управления замком двери, не более, В	30
Ток коммутации контактов электромагнитного реле управления замком двери, не более, А	2
Интерфейс для подключения ПЭВМ	RS-232
Чувствительная площадь сканера изображения отпечатка пальца, мм	14.2x0.4
Качество сканируемого изображения отпечатка пальца, dpi	500
Форма хранения в БД биометрической информации о пользователе	Шаблон размером 384 байта
Допустимый ток внешней нагрузки (питание дополнительного УСК, питание электромагнита дверного замка, питание кнопки выхода), при максимальном напряжении, не более, А	1.35

2. Шифроустройство для систем контроля и управления доступом У024-1 ЯЛКГ.425723.002 ТУ

Совмещенные считыватели бесконтактных карт доступа и биометрических признаков (отпечатков пальцев). Сфера применения та же, что и у считывателей карт доступа, совмещенных с клавиатурой.

Считыватель предназначен:

- для организации прохода в особо охраняемые помещения;
- для организации управления системами безопасности и жизнеобеспечения — там, где требуется дополнительное подтверждение принадлежности данной карты настоящему владельцу.

Дополнительная идентификация пользователя по биометрическим признакам в общем случае более надежна, нежели набор pin-кода: если пользователь системы проявил неосторожность, злоумышленник может подсмотреть pin-код.

Использование совмещенной технологии считывания бесконтактной карты и отпечатка пальца позволяет достичь более высокой скорости идентификации пользователя, что повышает пропускную способность точки доступа системы контроля управления и контроля доступом (СКУД), оборудованной таким считывателем, или повышает оперативность управления системами ОПС и жизнеобеспечения.

Принцип работы считывателя:

Считыватель имеет собственную базу данных (БД) пар «отпечаток пальца пользователя — карта пользователя», которая может быть создана непосредственным занесением в считыватель или передана в считыватель по последовательному интерфейсу.

В случае совпадения предъявленной карты доступа и отпечатка пальца с хранимой в БД считывателя парой на выходной интерфейс считывателя передается номер предъявленной карты. Таким образом, по выходному интерфейсу считыватель абсолютно схож с обычным считывателем карт доступа, что позволяет без проблем использовать его в существующих СКУД и системах управления ОПС.

В случае, если соответствующая пара не обнаружена, считыватель, в зависимости от настроек, может либо ничего не передавать на выходной интерфейс, либо передать специальный код, который может быть воспринят системой как предупреждающий сигнал (попытка доступа на особо важный объект или попытка управления).

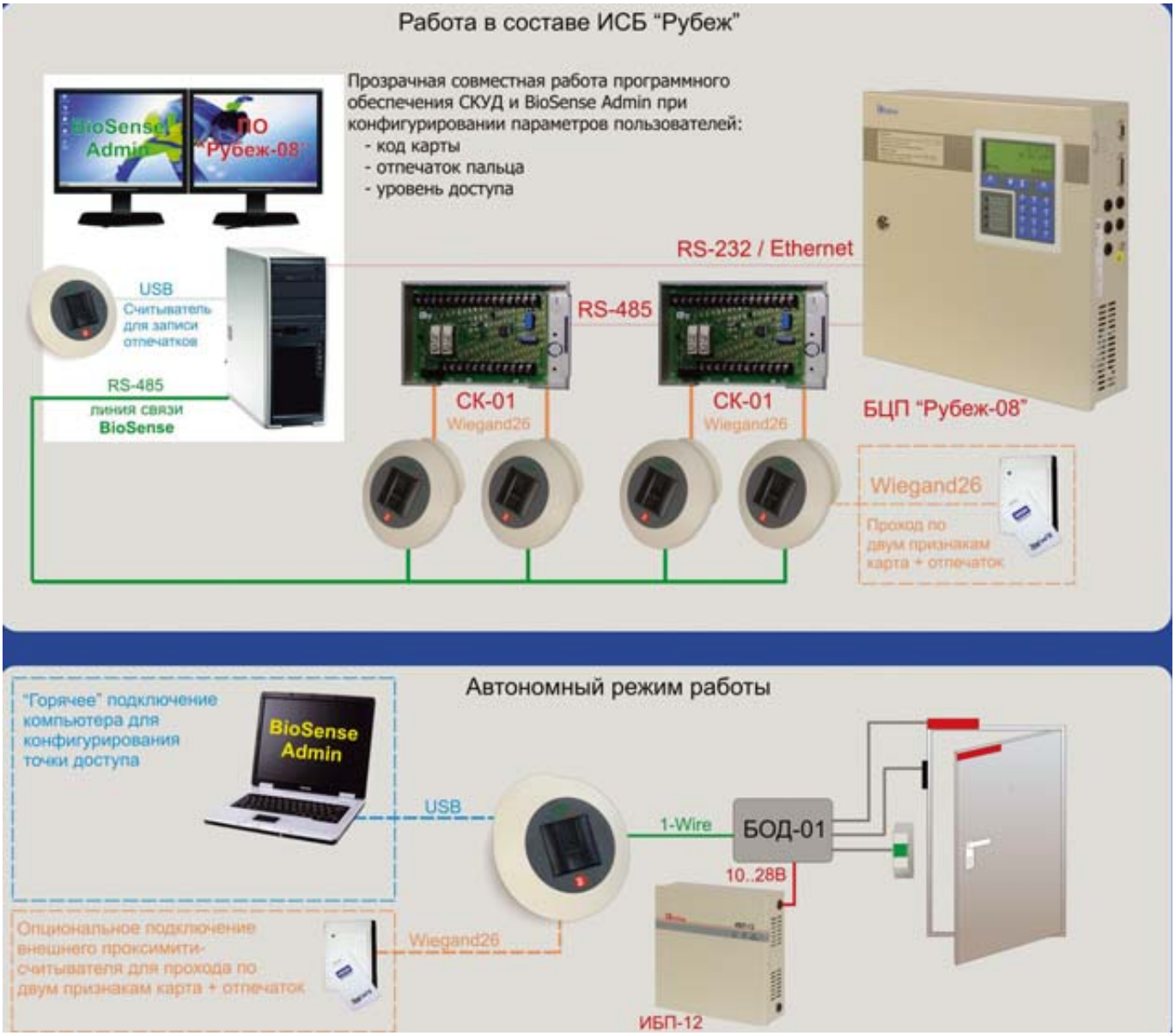
Характеристики:

- Количество отпечатков в БД считывателя — 1000.
- Дальность считывания карт — 10–12 см.
- Выходной интерфейс — Wiegand 26/40.

На рисунке 4 приведены схемы построения сетевых и автономных устройств контроля доступа на базе биометрических считывателей.

Для обеспечения контроля доступа на крупных объектах необходимо обеспечивать гибкий подход к построению структуры системы. При этом необходимо использовать как биометрический контроль доступа, так и другие виды идентификации (кодовые панели, карты RFID, электронные ключи). Это позволяет гибко подойти как к организации необходимого режима доступа с учетом требований высокой степени защиты от несанкционированного доступа, так и к обеспечению необходимой пропускной способности в точках доступа, а также обеспечить многорубежный контроль.

Рис. 4.
Структурная схема построения сетевой и автономной СКУД на базе биометрических устройств ШУ024-2



Для таких задач подходят специализированные сетевые СКУД.

Структура такой СКУД, сочетающей биометрический контроль с другими видами идентификации, приведена на рисунке 5.

Система контроля доступа «Senesys» предоставляет широкие возможности по обеспечению безопасности объекта за счет:

- организации пропускного режима и контроля доступа;
- решения вопросов управления персоналом.

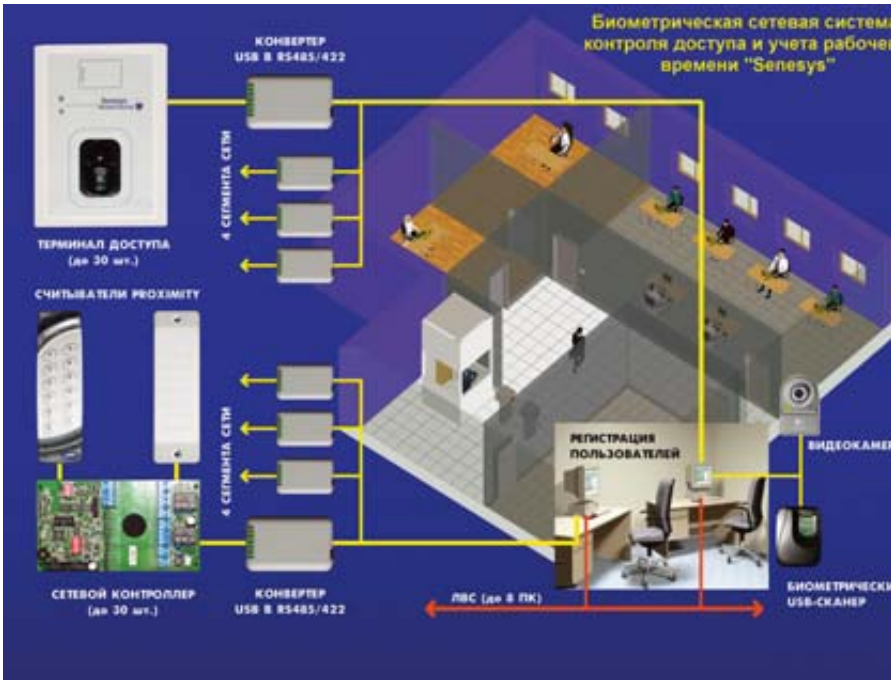


Рис. 5.
Сетевая СКУД «Senesys»

СКУД «Senesys» отвечает требованиям, предъявляемым к оборудованию и программному обеспечению современных систем безопасности, благодаря:

1. Комплексной идентификации клиента системы доступа по совокупности признаков;
2. Применению в СКУД современной биометрической технологии **FINGERPRINT;**
3. Универсальному модульному принципу построения;
4. Простой и быстрой процедуре первичной регистрации клиента системы контроля доступа;
5. Гибкости настроек для обеспечения требований повышенной безопасности;
6. Привлекательной цене.

Технические характеристики СКУД «Senesys»:

- идентификация пользователя по совокупности или устанавливаемому сочетанию следующих признаков: отпечаток пальца, проксимити — карта, индивидуальный PIN-код;
- количество Терминалов доступа Senesys в одном сегменте сети до 31;
- количество сегментов сети на один Управляющий компьютер — до 8;
- количество пользователей до 30 000 чел.;
- вероятность ложного распознавания отпечатка пальца (FAR — False Acceptance Rate) задается от 10–3 до 10–9;
- программная среда сервера Win2000/WinXP;
- исполнительный механизм — электромеханический замок или защелка, турникет, шлагбаум;
- электропитание периферийного оборудования 12 В.

Возможности и состав программного обеспечения СКУД «Senesys»:

1. обмен данными между Управляющим компьютером и Терминалами доступа «Senesys»;
2. наглядный и удобный мониторинг событий с возможностью их просмотра в реальном времени;
3. регистрация тревожных событий;
4. отображение состояния дверей, персональных данных пользователя при его идентификации;
5. база данных персонала (электронная картотека) с модулем регистрации клиентов системы контроля доступа;
6. модуль присутствия и табельного учета рабочего времени. Кроме того, программное обеспечение СКУД предоставляет различные фильтры событий и получение отчетов по совокупности задаваемых параметров.

Рамки статьи не позволяют более подробно остановиться на других технологиях биометрической идентификации, которые сейчас также бурно развиваются и внедряются в разработки.

Подводя итоги, можно отметить, что современные технологии идентификации, применяемые в СКУД, могут обеспечить автоматизированную защиту от несанкционированного доступа на объектах особой важности и повышенной опасности. Оптимальный эффект может быть достигнут с использованием системного подхода, реализуемого в рамках применения ИСБ в качестве технических средств обеспечения безопасности.