УДК 621.398

Анализ состояния и перспективы развития систем контроля и управления доступом в России

© П.Д. Иванов, И.Д. Суверина

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Сформулированы основные цели и задачи системы контроля и управления доступом (СКУД). Показаны типовые структуры СКУД. Проведен сравнительный анализ различных вариантов реализации СКУД, даны основные рекомендации по выбору средств и систем контроля доступа. Сделаны выводы о преимуществах внедрения СКУД для обеспечения безопасности предприятий, дана оценка перспективам их развития.

Ключевые слова: *информационные технологии, системы безопасности, управление доступом, идентификация, аутентификация.*

Защита любого объекта включает несколько рубежей, число которых зависит от уровня режимности объекта. При этом во всех случаях важным рубежом является система контроля и управления доступом (СКУД) на объект. Хорошо организованная, с использованием современных технических средств, СКУД позволяет решать целый ряд задач, таких как противодействие промышленному шпионажу, защита конфиденциальной информации, учет рабочего времени, контроль прихода и ухода сотрудников. При реализации конкретных СКУД используются различные способы и реализующие их устройства для идентификации и аутентификации личности.

СКУД — один из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом. По данным ряда экспертов, ежегодный прирост рынка СКУД составляет более 25 %. Число специалистов, работающих в сфере технических систем безопасности, превышает 500 тыс. человек [1].

Индустрия безопасности сегодня развивается семимильными шагами. Это связано с ростом мировой экономики, а также с подъемом в отдельных отраслях, проявляющих интерес к такого рода системам. Примерами таких отраслей могут служить розничная торговля, транспортная сфера, строительство.

Стремление руководителей избегать проблем бизнеса заблаговременно приводит к решению максимально обезопасить себя и свою компанию. Основной потребностью безопасной жизнедеятельности при этом является своевременное обладание объективной и точной информацией. Мониторинг, учет посещений, ведение базы данных и другие процессы выступают основными средствами обеспечения безопасности, в частности, в системах контроля и управления доступом.

СКУД — совокупность программно-технических и организационно-методических средств, с помощью которых решаются задачи контроля и управления помещением предприятия, а также оперативный контроль за передвижением персонала и временем его нахождения на территории предприятия [2].

Основная задача СКУД — управление доступом, ограничение доступа на определенную территорию, а также идентификация лица, имеющего доступ на проход.

Дополнительные задачи:

- учет рабочего времени;
- расчет заработной платы (при интеграции с системами бухгалтерского учета);
- ведение базы данных (БД) персонала/посетителей;
- интеграция с общей системой безопасности:

○ системой видеонаблюдения для совмещения архивов событий, передачи извещений о необходимости старта записи, поворота камеры для записи интересующего события;

○ системой охранной сигнализации (СОС) для автоматической постановки/снятия с охраны, ограничения доступа в помещения, поставленные на охрану;

○ системой пожарной сигнализации (СПС) для получения извещений о состоянии извещателей, автоматической разблокировки эвакуационных выходов в случае пожарной тревоги.

Системы контроля и управления доступом как компоненты систем безопасности прочно завоевали свою нишу на мировом рынке. По оценке компании General Electric, одного из крупнейших производителей средств и систем безопасности, объем мирового рынка безопасности ежегодно растет на 7–12 %. Активное развитие рынка СКУД с 1990-х годов в России также показало перспективность этого направления.

Рынок СКУД в России на данный момент достаточно обширен и весьма разнообразен, при этом он постоянно расширяется и обновляется. Сегодня на него приходится примерно 15 % отечественного рынка систем безопасности. На нем представлены как отечественные, так и зарубежные производители.

Продукция отечественных производителей составляет, по некоторым оценкам, 70 % от общей массы. Она не уступает зарубежной, а по многим параметрам даже превосходит ее. Российские производители разрабатывают и выводят на рынок очень интересные решения, которые обеспечивают широкий функционал и высокие показатели надежности систем безопасности. Компании, работающие преимущественно с некрупными СКУД, обеспечивают создание бюджетных систем с достаточно широким функционалом. Ведущие производители предоставляют продукты и для крупных потребителей, которым требуются СКУД с централизованной или смешанной архитектурой.

Такие системы с многоуровневой архитектурой позволяют обеспечить необходимый диапазон масштабирования и расширения функциональных возможностей.

Характерными чертами российского рынка в данной сфере являются четко выраженная фрагментарность, затрудненность оценки из-за различных оснований для сегментации, ограниченный доступ к информации, преобладание малых и средних компаний, высокий удельный вес высокотехнологичной продукции, зависимость от государственных заказов и слабая прогнозируемость доходов.

Будучи неотъемлемой частью систем безопасности, СКУД обладают значительным потенциалом. Они способны взаимодействовать и интегрироваться с другими информационными системами, обеспечивающими жизнедеятельность зданий и управление компанией в различных сферах ее деятельности. Речь идет о системах управления зданием, системах управления персоналом и коммерческих системах.

От других систем СКУД отличается непосредственным взаимодействием с пользователями. Получая исчерпывающую информацию о действиях персонала и посетителей (в том числе от других систем безопасности), они могут обмениваться ею с другими системами здания. Это позволяет в значительной степени упростить работу, а собственникам — получить значительную экономию ресурсов.

Например, реальные данные о времени прихода/ухода работников позволяют регулировать освещенность и микроклимат на рабочем месте. С учетом значительного вклада этих систем в энергопотребление (до 60 %) экономия от внедрения подобных алгоритмов может составить порядка 10–15 %.

Эти же данные, обработанные для бухгалтерских и кадровых служб, позволяют автоматизировать процесс расчета заработной платы, периодов отпусков, вести учет и анализ посещаемости по каждому сотруднику в отдельности. В результате уменьшаются расходы на содержание бухгалтерского аппарата, и повышается управляемость предприятием.

Унификация технологий карт в СКУД позволяет на уровне карты интегрировать коммерческие и социальные приложения, например, внутреннюю расчетную систему, медицинскую информацию о сотруднике, электронный кошелек и пр.

В самом простом случае такая система включает компьютер со специально написанным программным обеспечением, регулирующим организацию рабочего места администратора СКУД, сетевой контроллер СКУД, аппаратные модули и оконечные устройства: приемники информации (считыватели) и исполнительные устройства (электромеханические или электромагнитные замки, шлагбаумы, турникеты) (рис. 1).

Для ответа на вопрос, как же менялись поколения технологий идентификации СКУД в России, совершим небольшой исторический экскурс.

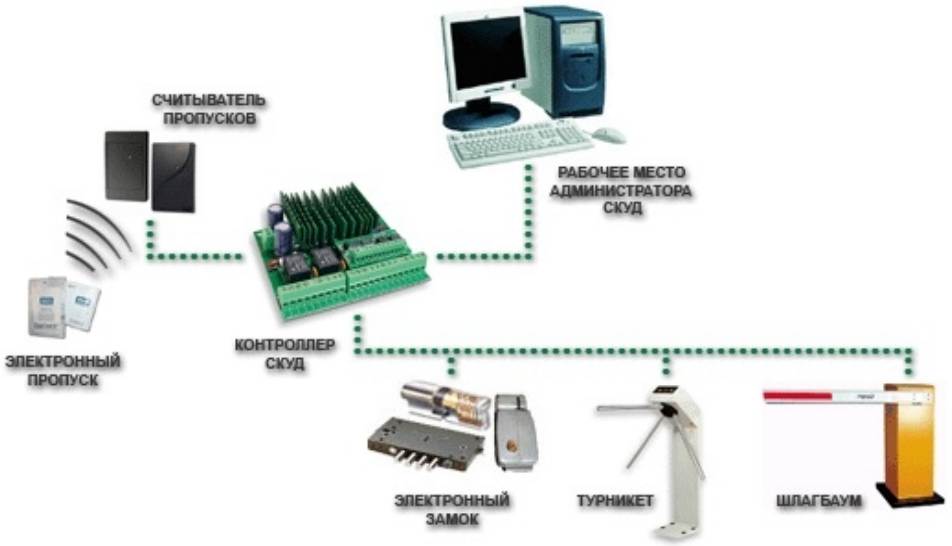

Рис. 1. Стандартная структура СКУД

«Первопроходцем» в России стала технология контактного типа. Это одна из первых технологий, которая была основана на магнитных картах. В данном случае технологическое отставание пошло нашей стране на пользу, так как к моменту проявления коммерческого интереса к СКУД со стороны российских потребителей в мире уже имелись более продвинутые технологии в этой области.

Магнитные карты и считыватели. Магнитные карты получили довольно широкое распространение в кредитно-финансовой сфере. Считывание данных происходит контактным способом — при проведении карты через считыватель. Использование в СКУД кредитных или дебетовых карт с магнитной полосой из-за некоторых технологических особенностей неоправданно, так как информация довольно легко поддается стиранию и перезаписыванию, что актуально для кредитных карт, однако совершенно недопустимо в СКУД.

Штрихкодовая технология. Штрихкод получил наибольшее распространение в системах торговли и складирования. В СКУД данная технология применялась редко из-за низкой степени защищенности от подделки: код можно отсканировать. Возможность перезаписывания и стирания информации также отсутствовала.

Wiegand-технология. Одним из способов устранения недостатков СКУД на основе магнитной и штрихкодовой технологий стала технология карт Виганда (Wiegand).

От магнитных карт Wiegand отличаются тем, что считывание карты происходит с помощью электромагнитного поля, индуцируемого считывателем. Карта Wiegand значительно долговечнее, так как при ее использовании отсутствует физический контакт со считывающей головкой, она устойчивее к механическим повреждениям, от-

вечает более высоким требованиям безопасности. Также следует отметить значительное увеличение температурного диапазона работы считывателей: от –40 до +70 °С. В качестве идентификаторов также могут использоваться ключи и специальные брелоки.

Таким образом, можно смело сказать, что данная технология стала переходной на пути к бесконтактным технологиям.

К достоинствам Wiegand-технологии можно отнести: небольшую стоимость, высокую защищенность от помех, устойчивость к механическим повреждениям, долговечность, надежность и хороший уровень безопасности.

К недостаткам следует отнести то, что это все же условно-контактная технология (карту необходимо проводить через считыватель), а также отсутствие возможности записи и невысокую пропускную способность.

Proximity-карты и считыватели. Одна из наиболее распространенных и эффективных технологий построения СКУД различного назначения — дистанционная радиочастотная Proximity-технология. Ее эффективность связана, прежде всего, с тем, что она не требует физического контакта между картой и считывателем.

Достоинства технологии Proximity: долговечность, надежность, устойчивость к механическим повреждениям, высокая пропускная способность; неограниченное количество считываний кода карты, возможности использования для учета перемещения не только человека, но и автотранспорта, широкий температурный диапазон, возможность использования совместно с другими технологиями идентификации.

Недостатки: невозможность перезаписи информации на карте, снижение дистанции чтения карты при нахождении рядом со считывателем силовых электрических установок и кабелей.

Последний недостаток привел к появлению новой технологии бесконтактной идентификации — Smart-картам и считывателям.

Бесконтактные Smart-карты и считыватели. Данная технология появилась сравнительно недавно, но уже успела завоевать огромную популярность в транспортной сфере. Главные признаки, отличающие эти считыватели и карты от обычных Proximity-устройств:

- наличие в карте большой области перезаписываемой памяти. Доступ к информации можно получить по специальному ключу;
- уникальный серийный номер (УСН) у каждой карты — гарантия того, что не будет выпущено двух одинаковых карт;
- довольно изощренный способ взаимной аутентификации, т. е. считывателя и карты, привязки карт к нужным считывателям.

В СКУД Smart-карты могут использоваться совместно с биометрическими считывателями. В некоторых областях Smart-карты уже активно используются, но в классических СКУД эта технология пока уступает Proximity. И все же можно уверенно сказать, что Smart — технология ближайшего будущего, идущая на смену Proximity.

Достоинства Smart: возможность перезаписи информации на карте с защитой от несанкционированного использования, взаимная аутентификация карты и считывателя, высочайший уровень безопасности, мультиаппликационность (возможность использования в разных приложениях помимо СКУД).

Недостатки: более высокая стоимость, чем у Proximity.

Биометрические технологии. Эти технологии подразумевают аутентификацию личности по строго индивидуальным биометрическим признакам человека (идентификаторам) (рис. 2).

Рис. 2. Индивидуальные биометрические признаки человека

В начале 1990-х годов биометрия в России не была изучена и стоила очень дорого. Тем не менее, в конце прошлого века некоторые российские компании уже предлагали биометрию заказчикам. Следует отметить, что к этому времени реальные характеристики считывателей стали намного лучше.

В 2000-х годах интерес к биометрии начал стремительно расти. Дактилоскопические считыватели (по отпечаткам пальцев) предлагались уже несколькими компаниями, но психологическая планка крайне высоких цен еще не была преодолена. В дальнейшем их стоимость снизили появление недорогих кремниевых сканеров и удешевление элементной базы.

Сегодня на рынке имеются биометрические устройства для верификации и идентификации пользователей по таким индивидуальным характеристикам, как отпечатки пальцев, черты лица, голос, радужная оболочка глаза, форма ладони, стиль набора на клавиатуре и подпись (рис. 3). Важно отметить, что все биометрические средства аутентификации в той или иной степени используют статистические

средства, имеющие вероятностный характер (см. таблицу). Это означает, что результаты их применения могут изменяться от раза к разу. Кроме того, подобные средства не застрахованы от ошибок [3].

Рис. 3. Способы биометрической идентификации

Сравнение современных методов биоидентификации [3]

Скорость идентификации	Дактилоскопия	Радужка	Лицо 2D	Лицо 3D	Рисунок вен
	Мгновенная	Мгновенная	Мгновенная	Средняя	Небольшая
Достоверность, % (вероятность ложного срабатывания)	0,001	0,00001	0,1	0,005	0,001
Стоимость, тыс. руб.	2–15	5–15	20–35	30–60	60–70
Сложность процедуры идентификации	Простая	Простая	Простая	Сложная	Простая
Адекватное количество персонала для применения данного метода, не более *N* человек	300	3 000	30	200	300

К достоинствам таких систем следует отнести возможность применения более сложных алгоритмов идентификации. Например, комбинированная биометрическая система аутентификации позволяет со-

единить несколько типов биометрических технологий в системах аутентификации в одной. Это позволяет удовлетворить самые строгие требования к эффективности. Аутентификация по отпечаткам пальцев может сочетаться со сканированием руки. Комбинированные системы более надежны с точки зрения возможности имитации биометрических данных человека, так как труднее подделать целый ряд характеристик, чем фальсифицировать один биометрический признак.

Очевидно, что стоимость, качество и надежность средств аутентификации должны быть напрямую связаны с важностью информации (рис. 4). Кроме того, повышение производительности комплекса, как правило, сопровождается его удорожанием [4].

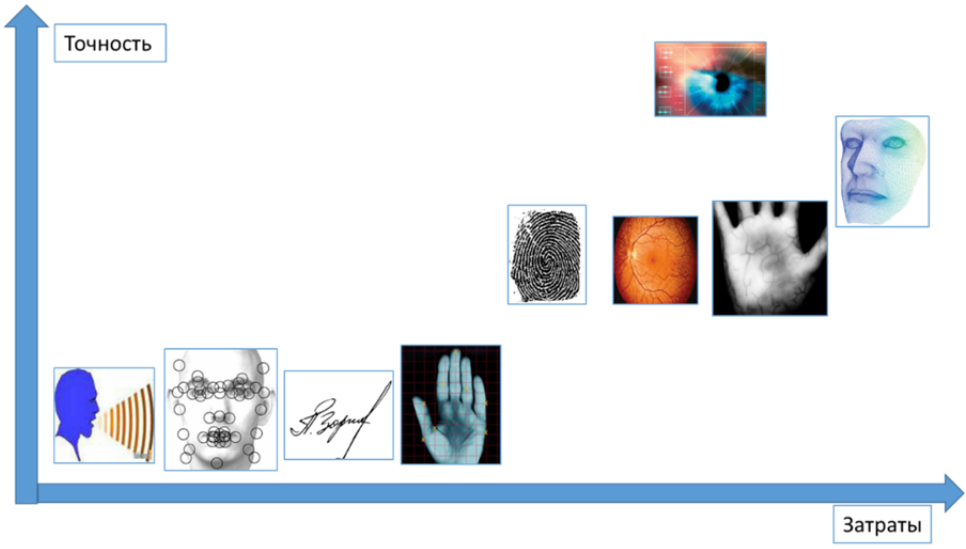

Рис. 4. Соотношение точности и затрат на применение метода [4]

Как же выглядит ситуация сегодня? Системы контроля доступа сегодня очень динамично развиваются. Предъявление высоких требований к надежности, простоте управления, легкости обслуживания, экономичности в работе и удешевлению базовой стоимости при увеличении функционала СКУД привело к появлению программно-модульных систем, которые обеспечивают гибкость при построении архитектуры каждого конкретного решения. При этом тенденция к созданию интегрированных систем, позволяющих в рамках СКУД объединять охранно-пожарные сигнализации, системы охранного теленаблюдения (CCTV) и обеспечивать диспетчеризацию контролируемых сооружений, привела к созданию действующих комплексных автоматизированных систем безопасности объектов.

Сейчас применительно даже к малым объектам можно смело говорить о комплексных системах безопасности и управления.

Главная из ожидаемых революций — появление облачных сервисов для учета рабочего времени — уже свершилась. В настоящий момент производители преодолевают первые серьезные проблемы на пути развития этого направления, которыми стали консерватизм конечных пользователей (сомнения в защищенности данных, хранящихся на «чужих» серверах) и строгая регламентация принципов защиты персональных данных со стороны Федерального закона № 152-ФЗ.

Можно с уверенностью сказать, что фактор максимальной открытости СКУД и учета рабочего времени в части интеграции с системами высокого уровня (ERP) останется одним из ключевых конкурентных преимуществ.

Перспективность и преимущества биометрических технологий создают впечатление однозначности и вседоступности. Однако все не так просто, как кажется на первый взгляд.

Грамотная разработка подразумевает большие затраты сил и средств, которые не каждое предприятие сочтет целесообразными. Сегмент СКУД сегодня прочно занят дактилоскопическими считывателями, которые просты в эксплуатации, недороги и многократно апробированы. Несмотря на их недостатки и достоинства других технологий, практика внедрения говорит за себя — пока это лидирующая технология.

Что можно сказать о перспективах? Уже сейчас отмечается тесная интеграция двух технологий — Smart-карт и биометрии. Наиболее реальными в перспективе представляются дальнейшая интеграция этих двух технологий и появление все большего количества устройств на их основе.

Параметры FAR и FRR дактилоскопических считывателей неидеальны. Например, идентификация по радужной оболочке или сетчатке глаза намного точнее, но пока существенно дороже. Очень интересно выглядят последние разработки в области 2D- и 3D-сканирования лица, интерес к которым проявляют как государственные, так и частные заказчики. К тому же бесконтактные технологии выглядят более перспективными.

С большой вероятностью можно сказать, что в ближайшее время развитие СКУД будет основываться на новых технологических решениях в области повышения функциональных возможностей периферийных устройств, а также совершенствования программного обеспечения.

В завершение отметим, что рост российского рынка систем безопасности стимулируется во многом теми же факторами, что и рост систем безопасности на мировом рынке. Из специфических благоприятных обстоятельств, для нашей страны аналитики отмечают хороший финансовый климат, рост культуры использования систем безопасности и увеличение доли российского производства.

Все больше направление развития СКУД зависит от конечного потребителя и требований, которые она будет предъявлять к безопасности, надежности и функциональности.

ЛИТЕРАТУРА

[1] *Средства и системы безопасности. Обзор рынка.* URL: http://stepconsulting.ru/publ/security.shtml (дата обращения 01.08.2014)

[2] Портной Евгений. *О некоторых особенностях систем контроля и управления доступом. Директор по безопасности,* 2011, № 10. URL: http://old.s-director.ru/magazine/archive/viewdoc/2011/10/374.html (дата обращения 01.08.2014)

[3] *Системы безопасности и видеонаблюдения.* URL: http://www.infotel-sec.ru/ (дата обращения 01.08.2014)

[4] *Магазин систем безопасности.* URL: http://www.safemag.ru/biometric-systems/ (дата обращения 01.08.2014)

Статья поступила в редакцию 28.08.2014

Ссылку на эту статью просим оформлять следующим образом:

Иванов П.Д., Суверина И.Д. Анализ состояния и перспективы развития систем контроля и управления доступом в России. *Инженерный журнал: наука и инновации*, 2014, вып. 10. URL: http://engjournal.ru/catalog/it/asu/1230.html

Иванов Павел Дмитриевич — аспирант, ассистент кафедры предпринимательства и внешнеэкономической деятельности МГТУ им. Н.Э. Баумана.
e-mail: ivanovpd@bmstu.ru

Суверина Ирина Дмитриевна — студентка кафедры предпринимательства и внешнеэкономической деятельности МГТУ им. Н.Э. Баумана.
e-mail: sid300993@mail.ru

Analysis of the state and prospects for the development of monitoring systems and access control in Russia

© P.D. Ivanov, I.D. Suverina

Bauman Moscow State Technical University, Moscow, 105005, Russia

Protection of an object consists of several lines, the number of which depends on the level of sensitive sites. In all cases, an important milestone is the system of access control systems (ACS). Well organized with the use of modern means access control allows to solve a number of problems, such as opposition to industrial espionage, protection of confidential information, time tracking, monitoring the arrival and departure of staff. With the implementation of specific ACS uses different methods and implement their devices to identify and authenticate a person. ACS is one of the most developed segments of the security market, both in Russia and abroad. According to some experts annual growth of ACS is more than 25%. The number of professionals working in the field of technical security systems, is more than 500 thousand people. In this article the main objectives and tasks of ACS are formulated, ACS typical structures are shown. A comparative analysis of the various embodiments of the ACS is made, basic guidelines for choosing the means and access control systems are provided. The conclusions about the benefits of implementing access control for enterprise security are reached and the prospects for their development are assessed.

Keywords: *information technology, security systems, access control, identification, authentication*

Ivanov P.D., postgraduate, assistant lecturer of the Department of Entrepreneurship and Foreign Economic Activities of the Bauman Moscow State Technical University.
e-mail: ivanovpd@bmstu.ru

Suverina I.D., a student of the Department of Entrepreneurship and Foreign Economic Activities of the Bauman Moscow State Technical University.
e-mail: sid300993@mail.ru