

Введение в системы контроля доступа

Системы контроля доступа (СКД) позволяют авторизованным сотрудникам получать доступ к различным компонентам вашего бизнеса, защищенным от остальных сотрудников компании. Размер системы может варьироваться от простой электронной кнопочной панели, защищающей одну дверь, до огромной системы, объединяющей группу зданий и включающую в себя контроль за парковочными местами, учет контроля времени и посещаемости и многое другое.

Использование современных систем контроля доступа является едва ли не обязательным в наше время. Система обеспечивает надежную защиту и является достаточно удобной. Вам не нужно будет заменять потерянные ключи, «охотиться» за уволенными сотрудниками и изымать у них ключи или просто гадать, кто имеет доступ к конкретной территории, а кто нет.

Перед покупкой системы

Перед тем как начать наводить справки о системе контроля доступа, серьезно подумайте о функции, которую она будет исполнять. Самая простая функция СКД — контроль доступа в определенные зоны. Это может быть парадная дверь, въезд на парковку, комната с компьютером-сервером или иная территория, нуждающаяся в экстрзащите. Все компьютеризированные СКД могут записывать кто, когда и где открывал определенную дверь. Вы можете использовать эти функции для автоматического контроля учета времени и посещаемости. Система не пропустит ни одного неавторизованного пользователя и в тоже время сможет производить учет рабочего времени. Для этого вам понадобится СКД, совместимая с программным обеспечением, ведущим учет времени.

Следующий момент, на который вам стоит обратить внимание это уровень безопасности. Насколько безопасной должна быть ваша система? Простенькая система обычно снабжена лишь кнопочной панелью или обыкновенной магнитной картой. Большой безопасности можно добиться с системами, которые требуют несколько видов идентификации (сочетание карт и отпечатков пальцев).

Решите также, какие еще системы будут соединены с СДК. Контролируемые противопожарные системы и ССТV являются хорошими примерами. Обязательно спросите у поставщиков оборудования обо всех требованиях, которые могут быть обязательными при соединении нескольких систем.

Размер системы

Как только вы решили, какую именно роль будет играть ваша СДК, решите, сколько дверей вам нужно охранять. Небольшие установки могут включать в себя только одну: серверная комната с электронным замком — пример очень маленькой СКД. Помните, что далеко не каждая дверь обязана быть включена в систему контроля доступа — вы можете просто оставить некоторые двери запертыми и отдать ключи нужным людям.

<http://www.hid.su> – системы контроля доступа HID (СКД, СКУД), бесконтактные смарт-карты, считыватели и программное обеспечение.

Если вы планируете все на шаг вперед, то вы обязательно подумаете о будущем расширении системы. Самые маленькие системы, предназначенные только для одной или двух дверей, трудно расширить, но несколько 4-х и 8 дверных систем могут быть легко объединены, если вам это потребуется.

После подсчета количества дверей, которое вы собираетесь охранять, соберите максимум информации о каждой из них. Есть ли двери, предназначенные только для работников или только для посетителей? Из какого материала сделаны двери – дерево, сталь или алюминий, стекло? Есть ли у вас дверь аварийного выхода? Нужно ли вам контролировать гаражные двери и ворота на паркинг-лот?

Большие установки могут состоять из нескольких частей. СКД, которая может управляться по сети, позволяет вам контролировать безопасность в любой ее части из центральной точки.

Свободный выход и системы контроля выхода

Еще один ключевой момент в СКД — разница между свободным выходом и системой контроля выхода. В системе со свободным выходом, нет никаких требований и ограничений к покиданию защищаемой территории. Система или улавливает того, кто приближается к выходу и открывает дверь или обладает специальной кнопкой или ручкой, которая позволяет людям покинуть здание.

Системы контроля выхода используют похожий принцип: работники должны ввести код или провести картой по считывателю, чтобы попасть внутрь или покинуть охраняемую территорию. По закону, СКД позволяют людям выйти из здания в случае отказа ее работы или отключения энергии. Системы контроля выхода повышают уровень безопасности, но с этим растут и ваши расходы.

Системы безопасности доступа

Система безопасности доступа может состоять из нескольких компонентов.

Определите для себя как вы хотите, чтобы система идентифицировала пользователя и открывала (или не открывала) для него доступ.

Кейпады (приборные панели) — это устройства, которые обычно используются для защиты одной двери или недорогой системы. Они просты в эксплуатации, но не обеспечивают большой безопасности. Пользователи имеют привычку записывать код где попало или «одалживать» свой пароль другим людям. Кейпады также не могут обеспечить вас подробным журналом контроля, если конечно вы не наградите каждого сотрудника персональным кодом доступа.

Считыватели карт это самое популярное решение проблемы контроля доступа в бизнес-системах. Они просты в эксплуатации, потерянные карты доступа легко деактивировать и произвести новые. Они могут быть также скомбинированы с фото для дополнительной безопасности.

<http://www.hid.su> – системы контроля доступа HID (СКД, СКУД), бесконтактные смарт-карты, считыватели и программное обеспечение.

Проксимити-карты способны работать на расстоянии от 3 до 90 см от сенсора-считывателя и являются очень популярными. Так как никакого контакта между картой и считывателем не происходит, проксимити очень надежны и смогут прослужить вам достаточно долго. К тому же они относительно недороги.

Существуют даже специальные проксимити-карты для автомобилей, которые позволяют получить доступ к парковке на расстоянии. Водителю не приходится открывать окно автомобиля или выходить из него. Автомобильные проксимити-карты могут работать на расстоянии нескольких метров от сенсора.

Системы безопасности доступа так же могут использовать и магнитные ленты, что поможет сэкономить вам деньги в том случае, если вы уже используете эти технологии для карт доступа своих сотрудников.

Биометрические системы полагаются на физические характеристики пользователей, используя для идентификации отпечатки пальцев, ладоней или даже сканируя сетчатку глаза. На данный момент эти устройства могут гарантировать максимальную безопасность. Впрочем, биометрические системы являются достаточно дорогими и не совсем надежны в использовании на улице.

Смарт-карты, в отличие от простых магнитных карт, могут содержать огромное количество информации, вплоть до состояния банковского счета или показаний медицинской карты.

Вам также будут нужны и электронные замки, которые будет контролировать система безопасности.

Программное обеспечение систем контроля доступа

Одно из самых больших различий между конкурирующими системами контроля доступа это компьютерное программное обеспечение, которое они предлагают использовать со своими продуктами. Эти программы позволяют вам установить уровни доступа для каждого ID и двери, просматривать отчеты и журналы контроля, чтобы узнать кто и когда использовал определенную дверь. Убедитесь, что вам легко работать с этими программами: системы контроля доступа должны помочь вам уменьшить количество проблем, связанных с безопасностью, а не принести еще больше. Попросите показать вам, как работает программа, насколько легко добавлять и удалять сотрудников из базы данных, менять уровень доступа, создавать группы и искать детализированные отчеты.

Убедитесь также, что это программное обеспечение подходит к вашей операционной системе — некоторые системы контроля доступа могут работать только с определенными версиями Windows или даже с другими ОС.

ASP

Вы можете решить использовать ASP (application service provider). Это провайдер, который будет работать с вашим программным обеспечением для контроля

<http://www.hid.su> – системы контроля доступа HID (СКД, СКУД), бесконтактные смарт-карты, считыватели и программное обеспечение.

доступа. Вместо того, чтобы загружать программы на ваш собственный компьютер, ASP или хостинговая компания работает с ними в своем собственном центре данных, а вы получаете доступ к нему через браузер.

Главным плюсом такого согласования является то, что ASP-центры могут обеспечить стабильную и постоянную работу вашей системы и вашим сотрудникам не придется работать с сервером, на который установлено программное обеспечение для контроля доступа. Впрочем, если у вас произойдет отключение интернета, вы не сможете сделать изменения в установке (система будет продолжать работать стабильно, но вы не сможете добавлять или удалять пользователей без подключения к интернету).

На наш взгляд, использование ASP является оптимальным выбором, если ваши сотрудники не являются экспертами в области СКД.

Также система контроля доступа может содержать различные дополнительные функции:

- контроль времени — позволяет вам установить нужное время блокировки и разблокировки дверей. В частности, это будет полезно, если у вас есть двери, которые открыты только для посетителей в одно время и только для рабочих в другое;
- генерирование отчетов — любая компьютеризированная система контроля доступа будет вести отчеты об использовании. Проверьте, какие именно виды отчетности может предложить система, и убедитесь, что она сможет обеспечить нужную вам детализацию;
- аварийное питание позволяет обеспечивать безопасность вашей системы в течение нескольких часов в случае проблем с подачей электроэнергии;
- печать бейджей — поставщик может обеспечить вас специальным принтером, так что вы сможете создавать новые карты, когда вам это будет нужно.

Какую фирму производителя системы доступа выбрать?

Мы рекомендуем тщательно подумать продукцию какой компании вам стоит приобрести. Компания-производитель должна обеспечивать постоянную техническую поддержку, занимать стабильные позиции на рынке и в тоже время ее продукция должна отвечать всем вашим потребностям. Лучшие компании-поставщики будут также задавать вам вопросы. Они объяснят как правильно пользоваться системой и постараются найти продукт, который оптимально подходит вашим требованиям. Не верьте менеджерам компаний, который заявляют, что у них есть «идеальная система контроля доступа для вас» после всего

<http://www.hid.su> – системы контроля доступа HID (СКД, СКУД), бесконтактные смарт-карты, считыватели и программное обеспечение.

лишь 5 минут разговора (к слову, на нее обязательно будет скидка и только на этой неделе.)

Большинство из производителей систем контроля доступа работают с разной категорией клиентов, но вы должны убедиться, что у них есть опыт работы именно в вашей сфере. Так, например, не стоит работать с компанией, которая специализируется на системах контроля доступа для частных домов, если вам нужна СКД для вашего бизнеса. СКД для частных домов в целом немного дешевле, но не стоит полагаться на них, так как они недостаточно надежны для использования в коммерческой среде.

Интеграция и инсталляция

В дополнении к нужной вам СКД и соответствующей технической поддержке, поставщик, которого вы выбрали, будет ответственен и за установку системы и ее интеграцию со всеми другими системами, которые у вас уже есть. Не существует реального стандарта совмещения контроля доступа и сигнализации и т. п. Ваш поставщик системы контроля доступа должен быть готов к этому и обладать опытом работы с системами, которые вы хотите соединить.

Сама установка может занять от двух дней до двух недель, в зависимости от общего числа ворот и дверей, которые будут контролироваться системой. Поставщик установит программное обеспечение на ваш компьютер (или покажет как соединиться с ASP), занесет первых пользователей в базу данных и установит нужное оборудование. Некоторые поставщики также предоставляют небольшой тренинг, включающий в себя навыки пользования программным обеспечением, информацией о создании карт и отчетов. Для работы с большими системами вам потребуется более полная подготовка.

В заключение хочется отметить, что для удачной покупки СКД, вам следует не забывать о нескольких простых правилах.

1. Оставайтесь на связи с вашим поставщиком после приобретения системы контроля. Это поможет вам решить множество проблем в дальнейшем.
2. Не забывайте, что многие замки обладают недостатками. В случае проблем с электроэнергией некоторые из них блокируют дверь изнутри, а некоторые наоборот полностью разблокируются. Вы должны решить, какие именно замки вам стоит использовать в той или иной ситуации.
3. Не забывайте, что вы можете использовать оборудование не один раз! Замки, сенсоры, считыватели или кейпады взаимозаменяемы между разными системами контроля доступа, так что все добавления и апгрейды могут добавляться к уже имеющейся базе.
4. Не покупайте слишком много. Установка защиты на каждую дверь вашего здания, скорее смутит ваших сотрудников, чем улучшит безопасность. Не думайте,

<http://www.hid.su> – системы контроля доступа HID (СКД, СКУД), бесконтактные смарт-карты, считыватели и программное обеспечение.

что вы обязаны включить каждую дверь в систему контроля доступа: комбинация карт доступа и обыкновенных старых ключей часто является лучшей комбинацией.

<http://www.hid.su> – системы контроля доступа HID (СКД, СКУД), бесконтактные смарт-карты, считыватели и программное обеспечение.