Multimodal Transport. (2019) IOP Conference Series: Materials Science and Engineering. 582, № 012038. DOI: 10.1088/1757-899x/582/1/012038.

СКУД ДЛЯ ОБЪЕКТОВ БАНКОВСКОЙ СФЕРЫ

О.С. Ковалева, студент гр. З-17Г51,
научный руководитель: Л.Г.Деменкова, ст. преп.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: olenka-shiryaeva@mail.ru

Аннотация: Системы контроля и управления доступом в банковской сфере являются важным средством обеспечения безопасности. СКУД позволяют защитить информацию, разграничив виды доступа в разные помещения банка. СКУД включают приборы для идентификации, ограничения доступа, управления и программное обеспечение. Рекомендуется интеграция СКУД с другими системами безопасности.

Ключевые слова: системы контроля и управления доступом, банки.

Системы контроля и управления доступом (СКУД) на объектах банковской сферы предназначаются для того, чтобы регулировать и контролировать вход/выход персонала и клиентов банка в его помещения. СКУД служит в качестве вспомогательного средства охраны и обычно интегрируется в системы охранно-пожарной сигнализации и видеонаблюдения объекта.

Как правило, перед СКУД в банках ставятся задачи обеспечения контроля за въездом/выездом автомобилей в том случае, если банк имеет собственный гараж; всеми существующими входами в помещение, на отдельные этажи (если здание банка многоэтажное), в помещения ограниченного доступа.

Здания банков как объекты для установки СКУД обладают определённой спецификой:

- имеются помещения, в которых осуществляются операции с клиентами, куда должен быть обеспечен свободный доступ посетителей;
- существуют помещения для руководства банка, где ограничивается доступ клиентов, а персонал банка передвигается согласно своих прав доступа;
- в наличии помещения режимного типа с доступом персонала согласно приказу.

Следует отметить, что при работе инкассаторской службы в банке современные СКУД могут временно остановить доступ персонала и клиентов в помещения, где находятся инкассаторы.

Независимо от специфических особенностей доступа в помещение банка, СКУД состоит из следующих компонентов:

- идентификационные устройства (биометрические сканеры, чипы, карты доступа и др.);
- устройства, ограничивающие доступ в помещения (турникеты, двери, замки);
- управляющие устройства (контроллеры, серверы);
- программное обеспечение (рис. 1).

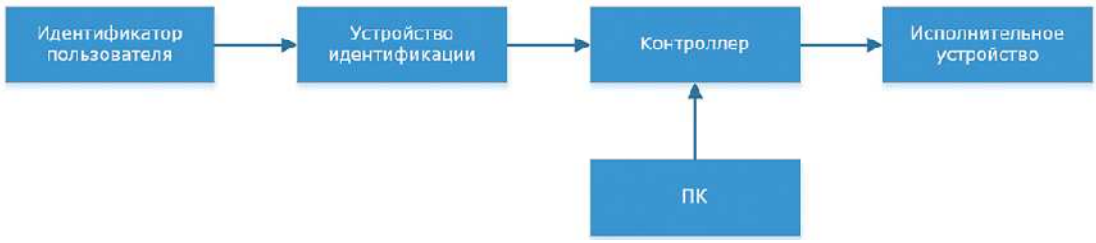

Рис. 1. Общая схема СКУД

Однако наличие специфических разноуровневых задач приводит к ряду особенностей. Например, в СКУД используются устройства, которые могут разблокироваться двумя способами: при подаче напряжения и при снятии напряжения.

В случае возникновения чрезвычайной ситуации при эвакуации работников и клиентов разблокирование дверей осуществляется либо в полуавтоматическом, либо в ручном режиме при использовании аварийных выключателей, а также с автоматизированного рабочего места охраны. Если

в помещении банка пропадает напряжение, СКУД автоматически переключается на резервное питание, обратный переход также осуществляется автоматически.

При проектировании СКУД объекта банковской отрасли руководствуются ГОСТ Р 51241-2008 "Средства и системы контроля и управления доступом" [1]; Р 78.36.005-2011 "Выбор и применение систем контроля и управления доступом" [2]. Согласно нормам, помещения банка делятся на три зоны. Доступ в первую зону ограничивается турникетом, дополнительные средства СКУД не используют, т.к. в первой зоне осуществляется работа с клиентами - физическими и юридическими лицами. Во вторую зону доступ осуществляется с помощью чипов, карт и т.п., иногда с помощью PIN-кода. Третья зона существует только в крупных банках и требует, как правило, биометрической идентификации.

Для выбора конкретной СКУД для банка следует учитывать, во-первых, её функционал, во-вторых, надёжность, а также возможность доработки под конкретные условия. Выбирая организацию для производства работ, обращают внимание на их опыт в данной сфере, анализируют готовые решения, произведённые подрядчиком, возможности сопровождения СКУД при эксплуатации.

Как отмечено рядом авторов [3-4], главная причина отказов СКУД при её эксплуатации - ошибки, допущенные при монтаже оборудования. Согласно теории надёжности, наибольшее число отказов наблюдается в начале эксплуатации, далее система работает довольно устойчиво, в конце эксплуатации число отказов увеличивается (окисляются контакты, выходит из строя электроника, появляются механические поломки деталей из лёгких сплавов и др.), и СКУД заменяют на новую. Это период, как показал опыт эксплуатации, занимает около восьми лет [5]. Для поддержания СКУД в работоспособном состоянии осуществляется её техническое обслуживание, ежемесячно проводится полное тестирование всех компонентов.

Анализируя статьи, посвящённые различным аспектам работы СКУД в банковской сфере [6-7], отметим, что СКУД должна быть надёжной, масштабируемой (т.е. иметь возможности к дальнейшему расширению и реализации других функций), создавать ограничения по доступу (временные и пространственные), контролировать передвижения персонала и клиентов, обеспечивать ведение электронной базы и архива сроком не менее 1 года. Надлежащее техническое состояние СКУД поддерживается за счёт оперативного вывода информации на рабочее место охранника/оператора/администратора. Электропитание СКУД в случае чрезвычайной ситуации обеспечивается за счёт источника бесперебойного питания, рассчитанного не менее чем на 24 ч работы. Для всех источников питания предусматривается заземление.

Прохождение персонала в режимные помещения, которые определяет приказ руководства банка (серверная, центр проведения платежей и т.п.) осуществляется с помощью дополнительных средств контроля доступа. К ним относятся, например, биометрические сканеры, определение сотрудника по фотографии, клавиатуры с персональным PIN-кодом и др.

Рассмотрим некоторые востребованные в реальной практике возможности СКУД [8]. Прохождение персонала и посетителей осуществляется через пост охраны. Здесь сканируется паспорт клиента, передаётся в базу данных, выдаётся электронный пропуск согласно цели визита и статусу клиента. Посетитель проходит через турникет и перемещается далее, используя полученный пропуск. СКУД отслеживает перемещения, контролируя определённые точки, при этом в режиме реального времени формируется отчёт. Для крупных банков востребована функция "Отчет по персоналу/рабочему времени", включающая информацию о времени прихода и ухода сотрудников, опозданиях и т.п.

СКУД может действовать как вспомогательное средство охраны, т.к. в некоторых СКУД реализована функция изображения контролируемых точек доступа (дверей) условными обозначениями, вид которых меняется в зависимости от её состояния (закрыта, открыта, взломана, идёт подбор электронного ключа и т.п.). Эта информация может помочь охране контролировать помещения, что особенно актуально в нерабочее время.

Решение проблемы устройства СКУД, которая была бы одновременно как надёжной, так и не слишком затратной по вложениям актуально практически для всех объектов банковской сферы. В современных условиях постепенно теряют свою значимость вещественные идентификаторы (карты, электронные чипы и т.п.), а также пароли доступа. Это связано с довольно значительными недостатками: всё вышеперечисленное можно потерять, забыть, передать другому человеку. Поэтому будущее систем контроля и управления доступом, как показано в работе [3], за использованием биометрических методов идентификации.

Список используемых источников:
1. ГОСТ Р 51241-2008 "Средства и системы контроля и управления доступом" [Электронный ресурс] // Викитека. - https://ru.wikisource.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_27593%E2%80%9488 (дата обращения: 16.02.2020).
2. Р 78.36.005-2011 "Выбор и применение систем контроля и управления доступом". - М.: НИЦ "Охрана", 1999. - 79 с.
3. Максимов, Р.Л. Разработка автоматической СКУД повышенной безопасности на базе типового решения СКУД BIOSMART с использованием автоматного подхода / Р.Л. Максимов, А.Г. Рафиков // Вопросы кибербезопасности. -2015. № 5(13). - С. 73-80.
4. Атаманов, Г.А. О банковской безопасности и безопасности банков / Г.А. Атаманов, Е.Г. Атаманов // Право и безопасность. - 2017. - № 1-2 (44). - С. 79-85.
5. Бужинская, Н.В. Система контроля и управления доступом на базе микроконтроллеров ARDUINO / Н.В. Бужинская, Е.С. Васева, Н.В. Шубина // Вестник Дагестанского государственного технического университета. Технические науки. - 2019. - № 46(1). - С. 103-112.
6. Ворона, В.А. Системы контроля и управления доступом / В.А. Ворона, В.А. Тихонов. - М.: Горячая линия-Телеком, 2010. - 272 с.
7. Волхонский, В.В. Системы контроля и управления доступом.- СПб.: Университет ИТМО, 2015. - 200 с.
8. Бадиков, А.В. Системы контроля и управления доступом / А.В. Бадиков, П.В. Бондарев. - М.: НИЯУ МИФИ, 2010. - 128 с.
9. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляе-мые. Общие технические требования. Методы испытаний. - М. : Стандартинформ, 2012. - 16 с.

ПОЖАРНАЯ БЕЗОПАСНОСТЬ СПОРТИВНЫХ КОМПЛЕКСОВ

В.В. Токарев, студент гр. 3-17Г51, научный руководитель: Л.Г.Деменкова, ст. преп.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail:vitalius@mail.ru

Аннотация: Статья посвящена проблеме пожарной безопасности на спортивных комплексах, актуальность которой возросла в последнее время в связи с ростом популярности занятий физической культурой и спортом среди населения в России и во всём мире. Спортивные комплексы вошли в жизнь современного человека. Обеспечение пожарной безопасности спортивных комплексов представляет важную задачу.

Ключевые слова: спортивные залы, пожарная безопасность, нормативная база.

В настоящее время резко возросла среди населения популярность фитнес-центров, спортивных и тренажерных залов. Все эти заведения должны системы противопожарной защиты, регламентируемые ФЗ-69 [1] и ФЗ-123 [2]. Согласно Постановлению Правительства РФ от 25 марта 2015 года N 272 [3] спортивные залы, в которых может находиться одновременно более 50 человек, относят к местам массового пребывания людей, что определяет меры пожарной безопасности.

По статистическим данным за 2019 г., основная причина пожаров во всех зданиях и сооружениях, в т.ч. и в спортивных залах, - неосторожное обращение с огнем (47000 случаев) [4]. Ещё на этапе проектирования спортивного зала добиваются, чтобы планировка всех помещений была проведена согласно строительным нормам, при этом применяемые отделочные материалы не должны быть огнеопасными, как регламентирует СНиП 21-01-97 [5].

В целях обеспечения пожарной безопасности в первую очередь руководителем назначается сотрудник, ответственный за пожарную безопасность. Если спортивный зал небольшой, руководитель может сам выполнять обязанности отслеживания соблюдения правил пожарной безопасности. Ответственный сотрудник (руководитель) проходит курс пожарно-технического минимума. Сотрудники, принятые на работу, обязаны пройти инструктаж по пожарной безопасности. Персонал должен знать, где расположены средства пожаротушения, уметь использовать их для тушения возникшего пожара. Работники должны уметь оказывать помощь посетителям спортивного зала при эвакуации. Далее инструктажи проводятся с периодичностью 1 раз в полгода. В случае изменения должностных обязанностей работники проходят внеплановый инструктаж. Даты фиксируются в журнале проведения инструктажей.