18 ноября 2020 г.

**Тема: «Технические средства видеонаблюдения (мониторинг, обнаружение, идентификации, распознавания). Система охранной сигнализации».**

**Литература:**

Т.С. Смирнова «Курс лекций по транспортной безопасности»

Эл. источник: «Транспортная безопасность» <https://e.lanbook.com/>

Домашнее задание:

Записать краткий конспект в свою тетрадь, пользуясь материалом лекции. Выучить, на следующий урок буду спрашивать.

Выполнить задания до 25 ноября 2020 г.

Задания выслать на электронную почту: **nata.kolovanchikova.80@mail.ru**

**Лекция**

**Безопасность это** - система, включающая в себя совокупность мероприятий, действий, документов и др., направленных на обеспечение защиты, комфорта жизни и деятельности человека, мест его проживания, работы, пребывания, а так же материальных, интеллектуальных и других ценностей, поэтому безопасность относят к базовым потребностям человека.

***Степень безопасность объекта характеризуется параметрами его защищенности от воздействия внутренних и внешних факторов***, при этом:

* под *объектом* понимается *территория, на которой необходимо обеспечить безопасность людей, материальных и информационных ценностей, целостность инфраструктуры объекта (*помещения, здания, сооружения, земельные участки и др.)*;*
* под *внешними факторами* мы подразумеваем *воздействие на объект из вне*, например несанкционированное проникновение (или попытка проникновения) на территорию посторонних лиц, транспорта, предметов и др.;
* под *внутренними*, *факторы действующие внутри объекта*, например нарушение работы различных систем (утечка воды, газа, отключение электроэнергии и др.), нарушение пользователями объекта прав доступа и др.

Для минимизации и устранения воздействия внешних и внутренних факторов, объект, в потенциально опасных зонах, оборудуется **инженерными средствами защиты**,  такими как *заборы*, о*граждения, решетки, ставни, замки, жалюзи, укрепленные ворота и двери, стены, потолки, полы, окна, воздуховоды и др. элементы конструкций*. Такие средства усложняют и замедляют проникновение нарушителя на территорию объекта, а так же заставляют лишний раз задуматься о целесообразности данного мероприятия. В совокупности с **техническими средствами** (например охранная сигнализация, [охранное видеонаблюдение](https://vashtvmir.ru/uslugi/videonablyudenie/)) увеличиваются возможности предотвращения проникновения, своевременного задержания нарушителя и компенсации причененного им ущерба. Применение таких технических средств, как системы СКУД, пожарная сигнализация, различные датчики и системы мониторинга, позволяют минимизировать риски и ущерб от внутренних факторов, например предотвратить пожар, своевременно обнаружить и принять меры по устранению утечек газа, воды, а так же ограничить несанкционированный доступ в отдельные помещения объекта и др. примеры. Следовательно,***уровень безопасности объекта зависит от наличия, обеспеченности и сочетания инженерных и технических средств защиты*,**то есть чем лучше они сочетаются между собой, дополняют друг друга, перекрывают “слабые места” объекта и учитывают его индивидуальные особенности, тем выше уровень защиты.

Все объекты обладают индивидуальными и присущими только им особенностями, поэтому требования к их уровню безопасности будут отличаться, так как один нуждается в более серьезной защите, другой в менее, акцент будет делаться на разные “слабые места”, будут усиливаться различные инженерные системы. Следовательно, в каждом конкретном случае, факторы, влияющие на целесообразность монтажа технологической системы безопасности, ее стоимость, функциональность, состав, структуру и взаимодействие с другими системами, будет меняться по степени воздействия и значимости. Приведем основные факторы:

* комплексная значимость объекта (в том числе его тактическая, стратегическая, культурная и др. ценность);
* требования к безопасности жизни и деятельности людей;
* вид, количество и степень значимости материальных и информационных ценностей;
* индивидуальные строительные и архитектурно-планировочными особенности;
* режим работы и функционирования объекта и др.

На основе пожеланий Заказчика и, с учетом вышеприведенных факторов, индивидуальных особенностей объекта, инженерных средств защиты, целесообразности,  и функциональности подбираются технические средства защиты объекта, которые могут относиться к разным системам обеспечения безопасности (охранная и пожарная сигнализации, видеонаблюдение, система мониторинга, контроль доступа и др.), но в своей совокупности образуют единый комплекс.  Таким образом:

1. ***Под технической защищенностью объекта понимается****совокупность мероприятий, направленных на усиление конструктивных элементов объекта (помещений, зданий, сооружений, заборов и т.д.) с целью обеспечения предотвращения и минимизации рисков несанкционированного проникновения, причинения вреда или ущерба людям, имуществу, объекту и иным ценностям.*
2. ***Под комплексной системой безопасности объекта (КСБ) понимается*** *совокупность различных систем (охранная и пожарная сигнализации, видеонаблюдение, система мониторинга и оповещения, контроль доступа и др.), направленных на обеспечение безопасности объекта в соответствии с требованиями и возможностями Заказчика, целесообразностью, индивидуальными особенностями объекта, инженерными и техническими характеристиками, степенью значимости, требованиями к уровню безопасности.*

***Системы обеспечения безопасности объекта, входящие в комплекс КСБ***, должны дополнять друг друга и взаимодействовать между собой в штатном режиме (без конфликтов оборудования и с минимальным коэффициентом ошибок). В современных комплексах безопасности объектов преимущественно (чаще всего встречаются) интегрированны следующие системы:

С помощью системы сбора и обработки информации с центральным пультом управления, отдельные системы объединяются в единый интегрированный комплекс системы безопасности объекта, дополняя друг друга и взаимодействуя между собой.

Классическая ***структура комплексной системы безопасности***включает в себя следующие элементы:

* *сервер* или основной (главный) компьютер для хранения, обработки и управления базами данных всех систем и аккумулирования отчетов;
* *рабочие станции* отдельных систем (если в них есть потребность) для обмена данными и командами с переферийными устройствами своих подсистем и предварительной обработки полученной информации (до передачи на главный сервер и обобщения);
* *переферийные устройства* систем (контроллеры, расширители, пульты управления и т.п.) для взаимодействия на аппаратном уровне со своими извещателями, датчиками, исполнительными устройствами, а на информационном уровне связывающими их по локальному интерфейсу (RS-485, RS-232) с рабочими станциями или сервером (шлавным компьютером);
* *извещатели* охранной, тревожной, пожарной сигнализации, считыватели, клавиатуры, видеокамеры, световые и звуковые оповещатели и т.д.;
* *локальная сеть Enternet* для обеспечения информационной связи отдельных систем, способных функционировать автономно, в единый интегрированный комплекс;
* *программное обеспечение* – сетевое, системное и прикладное  для сервера и рабочих станций, *микропрограммное обеспечение* для системных контроллеров, контрольных панелей и модулей;
* система гарантированного электропитания для обеспечения бесперебойного электропитания систем в случае возникновения внештатных ситуаций и перебоев с электропитанием

***Технические средства защиты объекта очень часто интегрируются с инженерными конструкциями и образуют единые инженерно-технические системы***, например:

* ограждение периметра территории объекта (сочетает в себе инженерные средства, например забор, и технические, например специальный кабель, датчики и др. оборудование);
* контрольно-пропускные пункты (турникеты, калитки, автоматические ворота, биометрические и карточные системы контроля доступа и др.);
* противотаранные устройства (дополняются камерами считывания номеров, считывателями, дистанционным управлением и др.);
* защитные ограждения помещений для хранения ценностей (в том числе спец.оборудование);
* сейфы, металлические шкафы и т.п. (например в сейфы оборудуются камерами видеонаблюдения, дополнительными замками и др.);
* оборудование внутренних постов охраны (броонекабины, турникеты, передаточные лотки и т.д.);
* специальные защитные ворота, калитки, двери (оборудуются дополнительными замками, автоматическими механизмами открывания, контроля доступа и др.);
* специальные защитные решетки, жалюзи, ставни для оконных проемов (оборудуются дополнительной автоматикой для управления, тревожными извещателями и датчиками и др.);
* защитные многослойные стекла (оборудуются датчиками вибрации, извещателями повреждения целостности стекла и др.) и т.п.

***Совокупность автономных инженерно-технических систем образует единую Комплексную инженерно-техническую систему безопасности объекта.***

**Средства и системы охранной, тревожной и пожарной сигнализации (ОПС)**

***Предназначены для выявления, своевременного информирования и пресечения попыток несанкционированного проникновения на охраняемый объект, а так же для обеспечения безопасности жизни и здоровья людей и предотвращения порчи имущества и иных ценностей от пожара, утечки газа, воды и др.***При возникновении внештатной ситуации (то есть при фиксировании датчиками отклонений от “нормы”), система подает сигнал тревоги и включает исполнительные устройства (световые и звуковые оповещатели, реле и т.п.).

Системы охранной и пожарной сигнализации получили очень большое распространение и применяются повсеместно на крупных объектах (заводы, производственные комплексы, склады, бизнесс-центры, крупные магазины), средних (офисы, многоквартирные дома, кафе, рестораны, фитнес-центры, гаражи, парковки) и маленьких (частные дома, квартиры, гаражные боксы, мастерские и др.). Такое распространение обусловлено высокой надежностью, эффективностью и экономичностью систем, так как автоматика не может вступить в сговор с охраной, отвлечься  и не подвержена иным “человеческим факторам”, но для определенных объектов, особенно крупных или с повышенными требованиями к безопасности, электронные системы обеспечивают повышение эффективности служб охраны, так как автоматика не может полностью заменить человека, обеспечить быстрое пресечение нарушений (например, когда большая территория и надо обезвредить нарушителей сразу, а не ждать прибытия спецподразделения),предусмотреть все внештатные ситуации и др.

В связи с тем, что охранная, тревожная и пожарная сигнализация очень близки по идеологии построения, то, как правило, на небольших объектах их совмещают на базе единого контрольного блока (приемно-контрольного прибора или контрольной панели).

**Системы ОПС включают в себя:**

* средства обнаружения и инициации тревоги – извещатели, датчики, в том числе дымовые, тепловые, пламени, газовые, ручные и т.п., кнопки, педали;
* средства сбора и отображения информации – ППК, контрольные панели, концентраторы, компьютеры, расширители, адресные и релейные модули;
* средства оповещения – световые и звуковые оповещатели, модемы и т.п.

***Извещатели – это устройства построенные на различных принципах действия и предназначенные для формирования определенного сигнала при соответствующем изменении контролируемого параметра окружающей среды***(колебание, изменение температуры, вибрация, уровень света и др.) и подразделяются на по области применения – на охранные, охранно-пожарные (практически не выпускаются) и пожарные:

* В свою очередь охранные извещатели делятся:
  + по виду контролируемой зоны – точечные, линейные, поверхностные и объемные;
  + по принципу действия – га электроконтактные, магнитоконтактные, ударноконтактные, пьезоэлектрические, оптико-электронные, емкостные, звуковые, ультразвуковые, радиоволновые, комбинированные, совмещенные и др.
* Пожарные делятся на извещатели ручного и автоматического действия, в том числе тепловые (реагирующие на повышение темпиратуры), дымовые (реагирующие на появление дыма), пламени (реагирующие на оптическое излучение открытого пламени), и др.

**Средства и системы охранного телевидения (видеонаблюдения)**

******Предназначены для обеспечения визуального контроля над всей территорией или определенными зонами объекта, фиксации и записи в архив передвижения людей, предметов, транспорта и др, обеспечения соответствующего функционирования других систем (контроль доступа, охрана периметра), с целью обеспечения защиты жизни и деятельности людей, сохранности материальных, информационных, иных ценностей, а так же инфраструктуры объекта.

**Принципиально системы видеонаблюдения можно разделить:**

* ***по принципу передачи видеосигнала и обработки информации на аналоговые, цифровые и гибридные***. Передача сигнала в видеонаблюдении основана на принципах передачи телевизионного сигнала в телевидении. Аналоговые системы (как и аналоговое телевидение) появились первыми и долгое время занимали лидирующие позиции, так как были первыми и доступней по стоимости, поэтому в настоящее время доля аналоговых систем видеонаблюдения остается достаточно большой. Цифровые системы видеонаблюдения отличаются большими возможностями, лучшим качеством изображения и большей функциональностью, но и более высокой стоимостью, однако, благодаря техническому прогрессу, возросшему спросу и высокой конкуренции, оборудование подешевело и стало активно вымещать аналоговые системы. Последнее время очень актуальным стало производить своего рода апгрейд (усовершенствование) ранее созданных систем (преимущественно аналоговых), так как цифровое оборудование (видеорегистраторы и др.) обладают большими возможностями, а производить полную замену оборудования системы (особенно если это большая система на крупном объекте) очень дорого, появился спрос на гибридное оборудование, таким образом образовалось новое направление развития, которое активно завоевывает рынок. Однако, скорее всего будет не очень продолжительным (относительное понятие) и продлиться до окончательного вымещения аналоговых систем, если конечно не изобретут новый способ передачи и обработки информации, тогда гибридные системы получат новый виток развития.
* ***по характеристикам передачи цвета на цветные или черно-белые***. Черно-белые системы получили очень большое распространение, так как появились первыми и были значительно дешевле цветных.  Цветные системы применялись когда цветное изображение несло существенную дополнительную информацию. Это было характерно для крупных объектов, на которых используется большое количество видеокамер и разница в стоимости была существенной, но в последнее время, стоимость оборудования стала ниже, доступность возросла и цветные видеокамеры стали постепенно вымещать черно-белые с рынка.

Еще одной из важнейших характеристик системы ОВН является ее разрешающая способность, т.е. возможность отображать наиболее мелкие детали изображения. Обычным разрешением считается 380-420 телевизионных линий для черно-белой видеокамеры и 300-350 для цветной (наша компания в своей практике применяет видеокамеры с более высоким разрешением от 600 до 800 твлиний). Видеомонитор должен иметь более высокое разрешение, чтобы не ухудшать общее разрешение системы. Целесообразно выбирать видеомонитор с разрешением 600-800 твлиний (мы применяем видеомониторы HD качества).

**Оборудование, входящее в систему охранного телевидения (видеонаблюдения):**

* телевизионные камеры (видеокамер);
* мониторы;
* оборудование для обработки изображений;
* устройства записи и хранения видеоинформации;
* источники питания;
* кабельные сети передачи информации и питания;
* дополнительное оборудование (термокожухи, поворотные устройства, ИК подсветка, прожекторы, дополнительные объективы)

Оборудование охранного телевидения (видеонаблюдения) коренным образом отличается от привычной бытовой техники. Например, мониторы обладают более высоким разрешением и надежностью, видеозаписывающие устройства – более плотной записью (от 24 до 960 ч.) и способностью изменять скорость записи по сигналу от внешних устройств, оборудование для обработки изображения (квадраторы, мультиплексоры, матричные коммутаторы) – выпускаются практически только для систем ОВН.

Широкий выбор оборудования, в различном ценовом диапазоне, разных производителей, качества, функционала и характеристик, заставляет задуматься при выборе не только простого обывателя, но даже профессионалов, а со временем перечень только расширяется. Чем больше выбор, тем конкретней и точней должно быть понимание, какую систему и для чего планируется создать. Поэтому, прежде чем преступить к выбору оборудования, необходимо четко определить задачи, которые она должна решить. Например:

* в каких условиях будет работать система- в помещении или на улице;
* климатические условия – температурный режим, климатические условия, особые условия (например порт, завод с вредной атмосферой, цех с повышенными темпиратурами или наоборот с очень низким диапазоном температур и т.д.)
* какое количество информации должна воспринимать, обрабатывать и хранить система;
* в каком режиме режиме – круглосуточно или только днем/ночью
* и много других, более узких и специализированных требований, как угол обзора, интеллектуальные функции и др.

Обеспечение безопасности объекта, особенно для служб безопасности и охраны, тесно связано со скоростью реагирования на возникновение внештатной ситуации. Только система охранного видеонаблюдения предоставляет возможность немедленно показать происходящие в данный момент событие, а не только предоставить информацию о месте и характере, как охранная, тревожная или пожарная сигнализация. Кроме того, система ОВН фиксирует все факты, сохраняет в архиве, обрабатывает и обладает другими важными и полезными функциями. Правильно спроектированная система позволяет в реальном масштабе времени сиюминутно оценить обстановку в контролируемых зонах, сократить время реакции на нештатную ситуацию и обеспечить принятие наиболее целесообразных мер защиты и противодействия возникшим обстоятельствам.

Можно выделить несколько основных задач, решаемых с помощью систем охранного телевидения:

* общее наблюдение за обстановкой;
* обнаружение появившихся в поле зрения видеокамер людей, животных, автотранспорта, предметов и т.п.;
* идентификация и сопоставление обнаруженных образов;
* фиксация и отслеживание траекторий движения обнаруженных объектов и др. функции.

**Системы видеонаблюдения (теленаблюдения)***подразделяются на простые (одна-две видеокамеры) и сложные (многокамерные) с различной обработкой изображений.*

* + *простые системы* применяются для текущего мониторинга за обстановкой на объекте в режиме реального времени, они не обладают специализированными функциями и состоят из видеокамер (одна или две) и видеомонитора, соединенных между собой линией связи для передачи сигнала от камеры на монитор. Такая система является базовой для систем видеонаблюдения любой сложности.
  + *сложные системы* – применяются на объектах с серьезными требованиями к безопасности или непосредственно к видеонаблюдению (например магазины и др.), включают в себя несколько  видеокамер, подключенных через коммутаторы, квадраторы или мультиплексоры на один-два видеомонитора. В среднем для таких систем используется до восьми видеокамер, так как большее количество усложняет работу одного оператора по мониторингу ситуации в каждой зоне наблюдения. Для одного оператора оптимальной нагрузкой считается наблюдение за изображением с четырех видеокамер.

**Системы видеоконтроля** – *позволяют осуществлять видеомониторинг за ситуацией на объекте, регистрацию и запись видеоинформации в архив на специальные устройства (видеорегистраторы, видеосерверы, “облако”)*, которые могут работать в непрерывном режиме или покадровой записи с заданными интервалами времени между кадрами, с обязательной записью текущего времени и даты. При воспроизведении такой записи возможен многократный ретроспективный контроль всей обстановки в подконтрольных зонах, детальное изучение тревожной ситуации с установлением времени происходящих событий.

*[](https://vashtvmir.ru/wp-content/uploads/2014/03/Arecont_Vision_SurroundVideo-1.jpg)*

**Системы видеоохраны** – или иными словами “зоны видеоохранной сигнализации”, это сложные системы охранного видеонаблюдения, инициирующие формирование сигнала тревоги при изменении видеоряда, поступающего с видеокамеры соответствующей зоны, то есть при изменении изображения, появления новых объектов или иных индивидуальных параметров, расценивающихся как отклонение от нормы (внештатная ситуация). Для этого в  системе применяется одно – и многоканальные детекторы движения.

****

*Детекторы движения бывают аналоговые* (преимущественно одноканальные) и *цифровые* (одно и многоканальные).

В аналоговых детекторах зоны, в рамках которых производится обнаружение движения, специально маркируются на видеомониторе белым или черным контуром. Для этого в каждом маркерном окне измеряется и отдельно запоминается среднее напряжение видеосигнала изображения (эталон) и затем, через определенный и заданный интервал времени, оно сравнивается с напряжением вновь поступающего изображения в тех же маркированных окнах. Если отклонение от эталона более определенного значения (обычно порог чувствительности 10%), то детектор движения генерирует сигнал тревоги.

В цифровых детекторах изображение на видеомониторе может разбиваться на несколько десятков или даже сотен маркерных зон (окон). Каждое окно может программироваться отдельно с присвоением индивидуальных параметров размера зоны и чувствительности (количество несовпадающих элементов и амплитуды несовпадений в каждом конкретном элементе). При этом все маркерные окна могут конфигурироваться в любом сочетании по желанию Заказчика.

Изображение в каждом маркерном окне каждого кадра одного цикла видеозаписи фиксируется отдельно в память цифрового детектора движения и затем, через установленный промежуток времени, сравнивается поэлементно с вновь поступающим изображением в тех же маркерных окнах в следующем цикле. При превышении заданного лимита несовпадении изображений в одном или нескольких одноименных маркерных окнах генерируется тревожный сигнал.

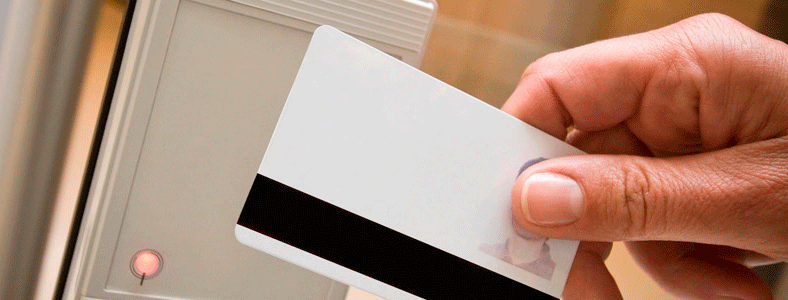
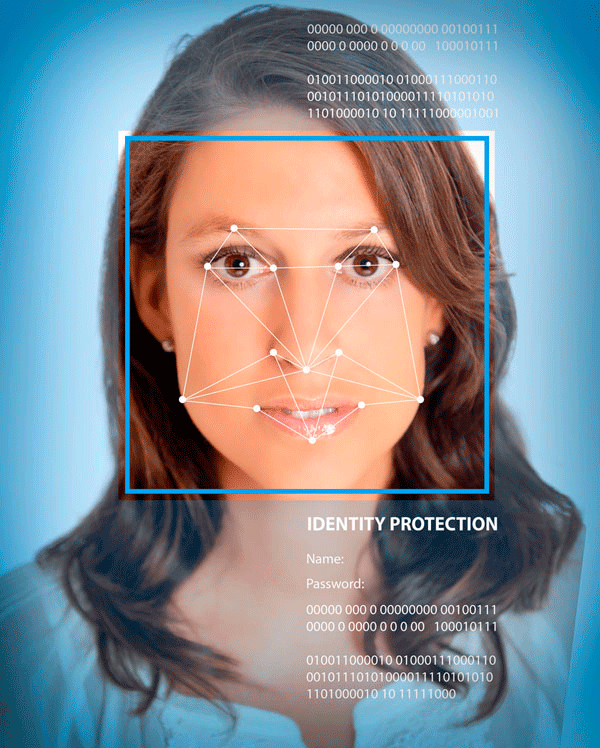
Набор параметров в дневное и ночное время на одном объекте может отличаться (например для супермаркета, торгового центра, офисного здания или склада), поэтому в детекторах задаются два переключаемых режима работы: дневной и ночной, отличающихся по конфигурации маркерных зон и по чувствительности. Режимы работы обычно переключаются с помощью внутреннего или внешнего таймера.

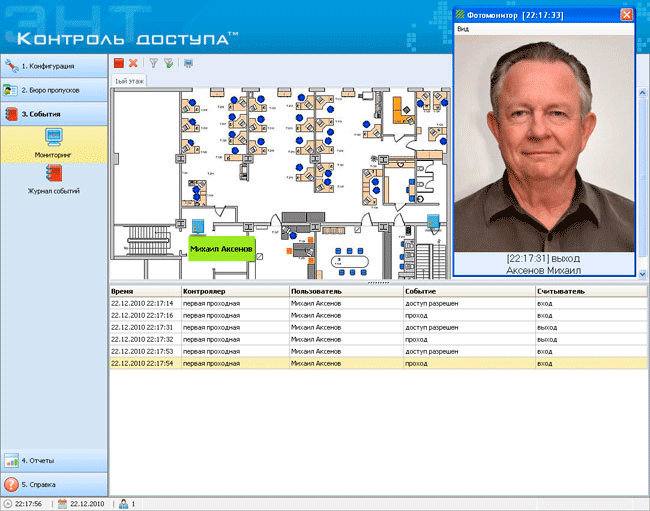
**[Средства и системы контроля и управления доступом](https://vashtvmir.ru/uslugi/kontrol-dostupa-skud" \o "Контроль доступа СКУД)**

*Системы контроля и управления доступом это совокупность программно-технических средств (оборудования и программного обеспечения) и организационно-административных мероприятий (законодательные, административные и нормативные документы, регламенты, инструкции и др., административные процедуры и др.), обеспечивающие организацию, ограничение, распределение и перераспределение прав доступа персонала, посетителей, пользователей (жильцов), транспорта на подконтрольную территорию объекта, с целью обеспечения безопасности жизни и деятельности людей, сохранности имущества, материальных и информационных ценностей, инфраструктуры и целостности объекта и др.*

В последнее время основной тенденцией развития СКУД является их интеллектуализация и интеграция с другими системами безопасности. В систему СКУД входит большое количество подсистем, которые могут работать полностью автономно ([домофон](https://vashtvmir.ru/uslugi/videodomofony), [турникеты](https://vashtvmir.ru/turniketyi-skud), [шлагбаумы](https://vashtvmir.ru/shlagbaumyi), [электронные замки](https://vashtvmir.ru/skud-zamki-kontrolleryi-dostupa-schityivateli-programmnoe-obespechenie), [автоматические ворота и калитки](https://vashtvmir.ru/avtomaticheskie-vorota-i-kalitki)и др.), а могут взаимодействовать со всеми системами контроля доступа и другими системами безопасности (например система проходной – взаимодействует оборудование СКУД:турникет, считыватели, контроллеры, программный комплекс и система видеонаблюдения: видеокамера и ПО, обеспечивающее дополнительно фиксацию, распознавание личности и запись факта прохода через проходную в архив).  Системы СКУД обеспечивают сбор, обработку и формирование отчетов с использованием значительного количества информации, и передают ее на главный компьютер (сервер), по сути, в комплексных системах безопасности, они выполняют одну из центральных функций, благодаря информации получаемой и передаваемой СКУД настраивается функции и регламент работы других систем, например видеонаблюдения, охранной и пожарной сигнализации, охраны периметра, освещения, вентиляции, отопления связи и др. (например, система СКУД сообщает, что сотрудник прошел через проходную на объект, система проверяет его права доступа и компетенцию, с охраны снимаются именно те помещения, в которые сотруднику разрешен доступ, автоматически подключается освещение в установленных помещениях, подключается отопление, в зависимости от количества пришедших сотрудников меняется режим работы вентиляции и др.).

**В состав программно-аппаратного комплекса СКУД  входит следующее оборудование:**

* ***Контроллер*** – высоконадежный электронный прибор, обеспечивающий аккумулирование, хранение и сопоставление информации о конфигурации и режимах работы системы, перечень лиц имеющих права доступа на объект и уровень их полномочий (в том числе [биометрические данные](https://vashtvmir.ru/biometricheskaya-sistema-kontrolya-i-upravleniya-dostupom-skud), для соответствующих систем). В простых системах, не требующих работы с большим количеством информации и разными функциями, контроллер может быть встроен в считыватель.
* ***Считыватели***(в том числе биометрические) – электронные устройства, отвечающие за извлечение (считывание) соответствующей информации с определенного носителя (пластиковые карты, штрих-коды, [биометрические данные-отпечатки пальцев, кистей, сетчатка глаза, черты лица](https://vashtvmir.ru/biometricheskaya-sistema-kontrolya-i-upravleniya-dostupom-skud) и др.) пользователя – личного идентификатора. Считыватель передает полученную информацию контроллеру, который производит сверку с хранящимися в нем данными и принимает решение о разрешении или ограничении доступа. В более масштабных системах эту функцию можно перенаправить на ПК, то есть окончательное решение о разрешении или запрещение прохода будет отдаваться с компьютера.
* ***Идентификаторы личности*** – носители информации о личности, полномочиях и правах доступа на объект конкретного лица. Вид и носитель идентификатора зависит от системы СКУД и параметров считывателя, например это могут быть ключи, брелки, магнитные карты, пропуска с штрих-кодом, а так же биометрические данные для соответствующих систем.
* ***Преграждающие устройства*** – это устройства, предназначенные для ограничения прохода или проезда на территорию объекта, которое освобождает проход или проезд только после подтверждения прав доступа посетителя и получения соответствующего сигнала от контроллера или компьютера. К таким устройствам относятся системы домофона и видеодомофона, электронные замки, шлагбаумы, автоматические ворота, калитки, турникеты, шлюзовые кабины и др.
* ***Устройства контроля и состояния преграды*** – датчики различных типов (например герконы), отвечающие за мониторинг состояния преграждающего устройства и передающие соответствующий сигнал в случае попытки несанкционированного проникновения (например открытия двери) и т.д.
* *****Блоки резервного и бесперебойного питания*** – предназначены для обеспечения работы системы в случае непредвиденного, аварийного или планового отключения основного электропитания.
* ***Программное обеспечение*** – необходимый элемент СКУД среднего и высокого класса, в то время как простые системы могут обходиться без него. Программный продукт устанавливается на компьютер и содержит аппаратные средства связи с контроллерами и обеспечивает выполнение важнейших функций по обслуживанию СКУД:
  + конфигурирование контроллеров с обеспечением процедуры занесения в них списков пользователей и их прав прохода;
  + ведение базы данных точек контроля прохода пользователей, допущенных в помещения и на территорию объекта, анализ их перемещений;
  + съем информации о событиях на точках контроля, ее обработка, документирование и архивирование;
  + предоставление оператору системы текущей информации;
  + оперативное управление системой и др.



Программное обеспечение является очень важной частью системы СКУД (кроме маленьких и не требующих аналитики, так как например даже система из двух считывателей будет нуждаться в ПО если Заказчик захочет вести учет рабочего времени), оно обеспечивает многие функции системы, облегчает работу с ней и позволяет взаимодействовать с другими системами. Именно поэтому сейчас многие разработчики ПО и оборудования разных направлений систем безопасности активно сотрудничают и интегрируют свои продукты. К сожаления, пока еще сохраняется ситуация, что программы управления СКУД от разных производителей ориентированы на управление линейками контроллеров конкретных производителей. Бывает, что для оборудования одного производителя несколько разработчиков пишут свое ПО. Однако, глобализация проект объективный, каждый производитель оборудования программного обеспечения и оборудования заинтересованы в его продвижении на рынке, поэтому создается все больше и больше интегрированных решений, что значительно расширяет возможности, функционал, органичность использования систем безопасности, а так же значительно облегчает монтаж, настройку и интеграцию систем.

**Средства и системы оповещения и управления эвакуацией людей при пожаре**

*Система предназначена для обеспечения своевременного оперативного оповещения и управления движением людей при эвакуации в безопасную зону, в случае возникновения пожара, внештатных ситуаций и иных угрозах для безопасности, жизни и здоровья людей. Безопасной зоной считаются помещения (или участка помещений) внутри зданий и сооружений и территория непосредственно объекта, прилегающая территория или помещения и территория, находящиеся на безопасном расстоянии от источника опасности, но не относящиеся к объекту охраны.*

Эвакуация обеспечивается согласно ГОСТ 12.1.004-91 по средством устройства необходимого количества эвакуационных путей с соблюдением требуемых параметров, а так же организацией своевременного оповещения людей и управления их движением.

Оповещение о пожаре или иных внештатных ситуациях осуществляется передачей световых (табло) и звуковых сигналов в помещения, где люди могут подвергаться угрозе, быть заблокированы в помещениях. Эвакуация сопровождается трансляцией речевой информации, содержащей инструкцию действий в соответствии с сигналом тревоги, направления движения, и т.д. Тексты специально разрабатываются и записываются заранее, содержат инструкции на разные случаи потенциальной опасности и включаются в четком соответствии с возникшей угрозой. Трансляция осуществляется через устройства громкоговорителей, система оповещения может быть совмещена с радиотрансляционной системой объекта. В этом случае элементы радиотрансляционной сети и помещение радиоузла должны удовлетворять предъявляемым к системе требованиям. Дополнительно пути эвакуации указываются специальными световыми табло, стрелками и надписями. Потенциально опасные зоны обозначаются табло или специальными лампами.

Система оповещения и эвакуации связана с системами пожарной сигнализации, выполняющей функции обнаружения источника пожара.

При проектировании и подборе оборудования системы оповещения и эвакуации, необходимо четко придерживаться требований нормативных документов – НПБ 77-98 (Нормы пожарной безопасности) и НПБ 104-03.

**В зависимости от функциональных характеристик СОУЭ (система оповещения и управления эвакуацией) подразделяется на пять типов:**

1. характеризуется наличием звукового способа оповещения (звонки, тонированный сигнал и др.);
2. характеризуется наличием звукового способа оповещения и светоуказателей “Выход” Оповещение должно производиться во всех помещениях одновременно;
3. характеризуется речевым способом оповещения (запись и передача спецтреков) и наличием светоуказателей “Выход”.  Регламентируется очередность оповещения: сначала обслуживающего персонала, а затем всех остальных по специально разработанной схеме и очередности;
4. характеризуется речевым способом оповещения (запись и передача спецтреков) и наличием светоуказателей “Выход”. Должна обеспечиваться связь зоны оповещения с диспетчерской. Регламентируется очередность оповещения: сначала обслуживающего персонала, а затем всех остальных по специально разработанной схеме и очередности;
5. характеризуется речевым способом оповещения (запись и передача спецтреков) и наличием светоуказателей “Выход”. Светоуказатели направления движения должны быть с раздельным включением для каждой зоны. Должна обеспечиваться связь зоны оповещения с диспетчерской. Регламентируется очередность оповещения: сначала обслуживающего персонала, а затем всех остальных по специально разработанной схеме и очередности Обеспечивается полная автоматизация управления системой оповещения и возможность реализации множества вариантов организации эвакуации из каждой зоны оповещения.

При оснащении объектов системами оповещения и управления эвакуации руководствуются индивидуальными параметрами объектов и четкими нормами регламентирующих документов, которые нужно неукоснительно соблюдать. Тип системы, структура, состав оборудования системы, его технические характеристики и др. определяются на основании нормативных документов и индивидуальны для каждого объекта, к этому вопросу нужно подходить очень серьезно, так как от правильности и эффективности работы системы (особенно на крупных объектах), могут зависеть жизни многих людей. Для маленьких и средних объектов чаще всего применяются 1 и 2 тип СОУЭ, для более крупных или сложных объектов остальные типы.