УДК 654.94
doi: 10.21685/2587-7704-2023-8-2-14

Open Access RESEARCH ARTICLE

Основные виды охранных систем

Татьяна Алексеевна Бубнова
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
abricos26@mail.ru

Екатерина Максимовна Мамина
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
m.ekat@mail.ru

Павел Геннадьевич Андреев
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
apg_58@mail.ru

Аннотация. Каждый человек хочет, чтобы он и все важные для него вещи находились в безопасности. Не исключение и крупные организации, которые хотят оставить свои разработки в секретности. Чтобы не допустить утечек информации и несанкционированных проникновений, существуют разные виды систем безопасности. Каждая из них имеет свои достоинства и недостатки и неповторимый принцип работы.

Ключевые слова: охранная система, сигнализация, видеонаблюдение, система контроля, управление доступом

Для цитирования: Бубнова Т. А., Мамина Е. М., Андреев П. Г. Основные виды охранных систем // Инжиниринг и технологии. 2023. Т. 8 (2). С. 1–6. doi: 10.21685/2587-7704-2023-8-2-14

The main types of security systems

Tatiana A. Bubnova
Penza State University, 40 Krasnaya Street, Penza, Russia
abricos26@mail.ru

Ekaterina M. Mamina
Penza State University, 40 Krasnaya Street, Penza, Russia
m.ekat@mail.ru

Pavel G. Andreev
Penza State University, 40 Krasnaya Street, Penza, Russia
apg_58@mail.ru

Abstract. Everyone wants him and all the things important to him to be safe. Large organizations that want to keep their developments secret are no exception. In order to prevent information leaks and unauthorized intrusions, there are different types of security systems. Each of them has its advantages and disadvantages, and a unique principle of operation.

Keywords: security system, alarm system, video surveillance, control system, access control

For citation: Bubnova T.A., Mamina E.M., Andreev P.G. The main types of security systems. *Inzhiniring i tekhnologii = Engineering and Technology*. 2023;8(2):1–6. (In Russ.). doi: 10.21685/2587-7704-2023-8-2-14

Введение

Актуальной проблемой современности является защита материальных и информационных ценностей различных организаций и сфер деятельности. Существующие виды охранных систем разнообразны [1, 2], имеют различные особенности применения и ценовой уровень. Постоянно разрабатываются новые охранные системы с более высокой степенью защиты от внешних воздействий с применением современных систем автоматизации исследования и проектирования радиоэлектронной аппаратуры [3–13].

Охранная сигнализация – это система, предназначенная для обнаружения вторжений, таких как несанкционированное проникновение в здание или другие помещения.

На сегодняшний день можно выделить следующие основные виды охранных систем:

1) системы, предназначенные для охраны и сообщения тревожных сигналов (СОТС);
2) системы, предназначенные для контроля и управления доступом (СКУД);
3) системы, предназначенные для обеспечения охранного видеонаблюдения (СОВН);
4) системы, предназначенные для обеспечения инженерно-технической стойкости объектов (СИТУ).

Рассмотрим каждый из этих видов более подробно, чтобы разобраться, какой вид охранной системы наиболее желателен для использования.

Для начала предлагаем обратить внимание на СОТС.

Система охраны и тревожной сигнализации

Данные виды систем позволяют осуществлять круглосуточный контроль за состоянием любого объекта. К таким объектам относятся офисы, склады, квартиры, коттеджи и т.д. На сегодняшний день системы охраны и тревожной сигнализации являются одним из самым надежным и повсеместно используемым способом для защиты охраняемых объектов от проникновения нарушителей.

Данные виды систем можно разделить на следующие типы:

1) пассивные системы охранной сигнализации;
2) системы активной охранной сигнализации.

Особенности первого типа в том, что при факте несанкционированного вторжения на территорию охранения сразу же выдается как звуковой, так и световой сигнал тревоги. Однако на диспетчерский пульт охраны информация о нарушении не поступает. Поэтому система оказывает на нарушителя только психологическое воздействие и в каких-то случаях может предотвратить дальнейшие противозаконные действия. Но, к сожалению, эффективность данной системы не всегда может быть высокой, особенно при охране особо опасных объектов.

Во втором случае объект охраны оборудуется датчиками, которые посылают сигнал тревоги на контрольную панель охраняемого объекта, и далее на пульт диспетчерской службы специализированной охранной организации. Пульт диспетчерской службы способен принимать сразу несколько сигналов от разных объектов охраны. Это позволяет определить место проникновения и принять быстрые меры реагирования.

К элементам каждой СОТС относят:

– датчики;
– центральное приемно-контрольное устройство;
– устройства оповещения – радио- и GSM-передатчики, светозвуковые устройства;
– пульт управления;
– устройство контроля состояния датчиков и кабельных линий в СОТС;
– источник питания.

Как уже было сказано ранее, основными отличительными особенностями и достоинствами систем СОТС является наличие датчиков. Они непосредственно должны отвечать за оперативное реагирование всей системы безопасности на вторжение. Рассмотрим более подробно данный вид систем.

Системы с инфракрасными датчиками движения, которые реагируют только на факт перекрытия инфракрасного луча нарушителем при любом перемещении в пределах объекта охраны. Они являются двухпозиционными, в их состав входит специальный инфракрасный передатчик и специальный инфракрасный приемник, который реагирует только на факт исчезновения сигнала, когда нарушитель перекрывает определенную оптическую ось датчика.

Система с емкостным датчиком позволяет создать в охраняемом помещении объекта электромагнитное поле с заданным значением емкости. Когда в помещение попадает любой предмет или нарушитель, поле меняет значение своей емкости. Этот факт вынуждает систему генерировать сигнал тревоги, пришедший от датчика.

Системы с проводноволновыми датчиками генерируют электромагнитное поле между двумя зонами, образованными проводниками, по которым передается сигнал. Датчик срабатывает в случае пересечения нарушителем или каким-то объектом этого поля. Следует отметить, что на факт движения реагируют также и другие виды систем, такие как системы с пассивными ИК-датчиками, радиолучевые и радиоволновые системы безопасности.

Системы с вибрационными датчиками, в случае нарушения охраняемой зоны, выдают сигнал тревоги на пульт охраны, однако вызван он возникновением вибрации. Можно выделить следующие

случаи возникновения таких вибраций: в случае разбивания оконных конструкций, при попытке проломить или пробить стену, при попытке вскрыть сейф или шкаф и т.п.

Системы с акустическим датчиком активно реагируют на наличие звука разбитого стекла, а также на любой другой громкий звук иного происхождения. Они также выдают сигнал тревоги на пульт охраны.

Системы с магнитоконтактными датчиками срабатывают и выдают сигнал тревоги при факте открытия окна, двери, крышки и других аналогичных конструкций.

Для более успешной работы СОТС в помещении желательно устанавливать не один, а несколько типов датчиков. Это позволит обеспечить более надежную защиту.

Следующей системой для рассмотрения предлагаем СКУД.

Система контроля и управления доступом

Данные автоматизированные системы предназначены и используются для обеспечения многоуровневой защиты от несанкционированного доступа на объекты охраны и в помещения, с учетом заранее заданных зон доступа, а также установленным уровнем идентификации лиц с заявленными правами доступа. Самым простым и широко распространенным примером данного вида системы безопасности является домофон. Как известно, он распределяет и ограничивает права доступа жильцам в подъезд многоквартирного дома. При этом наличие электронного ключа доступа является разрешающим фактором.

Системы СКУД обычно состоят из следующих составных частей:

– модуль, содержащий контроллер или их набор;

– модуль, содержащий считыватель информации;

– модуль, содержащий идентификатор информации;

– исполнительное устройство или их набор.

При этом в микроконтроллере должна храниться информация о всей конфигурации системы контроля и управления доступом и объекте охраны. Кроме того, в нем хранится информация о текущем и возможном режимах работы системы СКУД. Там же находится информация о имеющихся правах доступа различных сотрудников, а также вспомогательная информация об объекте охраны. Модуль, содержащий считыватель, должен получать информацию, которая записывается непосредственно в модуле идентификатора, а далее вся информация должна передаваться в контроллер для дальнейшей обработки.

Следует отметить, что под идентификатором может пониматься электронный ключ с различным формфактором, а также пластиковая карта доступа, снабженная микрочипом. Во многих системах СКУД применяются биометрические терминалы. Они призваны идентифицировать человека по отпечаткам его пальцев или считывании информации с глаза по радужной оболочке. Следует отметить, что на сегодняшний день большинство из перечисленных идентификаций уже получили широкое распространение и применяются в повседневной жизни.

По окончании процесса идентификации микроконтроллер подает соответствующую команду на исполнительный механизм или исполнительное устройство. После этого происходит разрешение или запрет на допуск в заданное помещение или объект. Под исполнительными механизмами и устройствами понимаются следующие виды изделий: замковые устройства, турникетные механизмы, различные приводные механизмы ворот, шлагбаумов и т.п.

Для обеспечения безопасности собственных объектов и материально-технических ценностей предприятия любых видов имущества используют цифровые СКУД, функционирование которых построено на сопоставлении идентификационных признаков посетителей с их учетными данными при помощи особых технических и программных средств.

Системы контроля и управления доступом осуществляют идентификацию и аутентификацию пользователей, получая и анализируя их учетные данные с помощью личных идентификационных номеров, биометрических показателей, электронных ключей безопасности, паролей или других факторов. Многофакторная идентификация/аутентификация, для которой необходимо два или более идентификационных признака, является важной частью многоуровневой защиты в системах контроля доступа.

На практике СКУД достаточно часто интегрированы в общую ИТ-инфраструктуру организации. Управляющая платформа СКУД обеспечивает взаимодействие специализированных программных модулей, базы данных, инструментов управления политиками контроля доступа, удаленного аудита и защиты информации.

В состав СКУД могут входить дополнительные технические средства, такие как источники электропитания, датчики состояния ПУ, доводчики, преобразователи интерфейсов, а также средства обнаружения опасных предметов и веществ (металлодетекторы, обнаружители взрывчатки, радиационных материалов и т.д.).

Данная охранная система хоть и перспективна в своем развитии, в ней присутствуют минус – она предназначена в основе своей для непропускания на охраняемую территорию или объект. Отлично, если при использовании данной системы решат использовать звуковой сигнал при несанкционированном проникновении, чтобы оповестить людей о попытке вторжения, чтобы задержать недоброжелателя. Но злоумышленнику не всегда необходимо всегда пробираться через парадную дверь, есть возможность найти обходной путь, и тут данная система уже не поможет.

Система охранного видеонаблюдения

Данная система охраны позволяет вести за объектом охраны постоянное видеонаблюдение с применением специальных камер. При этом возможна организация такого наблюдения одновременно за несколькими объектами. Так, например, под главным объектом наблюдения можно понимать главный вход, а под дополнительным – отдельные вход в дом, ворота, часть периметра охраняемого объекта или его отдельные помещения.

Главной задачей таких систем является необходимость обеспечения безопасности посредством визуального наблюдения, а также возможность получения актуальной информации об объекте в режиме онлайн. Кроме получения реальных данных система позволяет выполнить анализ случившихся событий по информации, которая была записана и сохранена на внутреннюю память или в облачное хранилище данных в интернете.

Можно выделить следующие типы передачи видеосигнала системы охранного видеонаблюдения:

1) проводные системы;
2) системы с беспроводной технологией.

Беспроводные системы можно устанавливать в самых труднодоступных местах, но зато проводные более надежны и дешевы.

Существует несколько видов камер СОВН. Все они подразделяются в зависимости от своих технологических характеристик. Две самые большие категории – это цифровые и аналоговые камеры.

Данные системы безопасности обладают простой и быстрой масштабируемостью, простой интеграцией в единую цифровую сеть, что является явным преимуществом этих систем. Кроме того, повышение цифрового разрешения используемых камер позволяет значительно увеличить значение цифрового увеличения или приближения объектов, что также является большим плюсом при обеспечении безопасности объектов.

Достоинством же аналоговых камер является использование специализированных интегральных микросхем – ПЗС-матрицы. Монохромные видеокамеры являются чувствительными не только к видимому, но и к невидимому – инфракрасному излучению.

Хоть данный вид охранной системы и легок в понимании и осуществлении, есть значимый минус по сравнению с предыдущими – большое влияние человеческого фактора. Если охранник проявит невнимательность или случится поломка камеры (случайная или запланированная), тогда злоумышленник сможет незамеченным пробраться в охраняемый объект. Нет стопроцентной гарантии такого сценария, но вероятность подобного, к сожалению, существует.

Система инженерно-технической укрепленности

Система инженерно-технической укрепленности, или же СИТУ любого здания, – это защита от несанкционированного проникновения путем усиления его конструктивных элементов.

Каждый знаком с данным видом защиты. Самый яркий пример такой защиты – это построение высокого и надежного забора на территории охраняемого объекта. В частных секторах любого города можно встретить дома с забором, который блокирует проход людям, не проживающим на данной территории.

Помимо заборов к данному виду можно отнести также ворота, пропускные пункты, шлюзы для проверки и пропуска транспортных средств.

Для защиты здания – оконные решетки и решетки для усиления стен, тамбуры, оснащенные средствами безопасности, укрепленные двери, замки.

В наилучшем случае необходимо устанавливать систему СИТУ в пять зон охраняемого объекта:

– первая зона – это периметр территории охраняемого объекта, который принимает первым нарушителя;

– вторая зона, которую составляет периметр всего здания охраняемого объекта;

– третья зона – это помещения здания охраняемого объекта, доступные только для посетителей;

– четвертая зона – это помещения здания охраняемого объекта, доступные только для хозяев дома;

– пятая зона – это помещения, оружейные и сейфовые области здания охраняемого объекта, обладающие максимально ограниченным доступом.

Заключение

Каждая перечисленная система охраны хороша по-своему, имеет разный принцип работы и выделяется на фоне других, но и у каждой есть свои минусы. И не удивительно, что самой распространенной является СОТС. По сравнению с другими видами, она меньше всего подвержена влиянию человеческого фактора для своего функционирования. В остальных случаях у злоумышленника есть шанс, что о его попытке проникновения даже никто не узнает; СОТС благодаря датчикам сразу доводит информацию для людей и если действовать оперативно, тогда преступника быстро удастся задержать на самом месте преступления. Но лучше всего, конечно же, комбинировать данные виды между собой, чтобы достигнуть наивысшей степени безопасности.

Список литературы

1. Львович И. Я., Воронов А. А. Применение методологического анализа в исследовании безопасности // Информация и безопасность. 2011. Т. 14. № 3. С. 469–470.
2. Рыжова В. А. Проектирование и исследование комплексных систем безопасности. СПб : НИУ ИТМО, 2013. 156 с.
3. Аполлонский С. М. Защита техносферы от воздействия физических нолей и излучений : в 3 т. Т. 3. Методы защиты от физических полей и излучений : монография. М. : РУСАЙНС, 2016. 336 с.
4. Andreev P. G., Yurkov N. K., Grishko A. K., Kochegarov I. I., Zhumabaeva A. S. Study of dielectric effect on signal propagation in the gigahertz range at elevated temperature // 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF 2019). 2019. С. 8840587. doi: 10.1109/WECONF.2019.8840587
5. Yurkov N. K., Andreev P., Bushmelev P. Space-time analysis of conductive paths with allowance for temperature influence // Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM. 2016. doi: 10.1109/SCM.2016.7519739
6. Mikheev M. Y., Roganov V. R., Andreev P. G., Goryachev N. V., Trusov V. A. Developing the structure of the quality control system of power supply units in mobile robots // 2017 International Siberian Conference on Control and Communications, SIBCON 2017 – Proceedings. 2017. С. 7998579. doi: 10.1109/SIBCON.2017.7998579
7. Grishko A. K., Kochegarov I. I., Lysenko A. V., Andreev P. G., Goryachev N. V., Danilova E. A. Determination of electromagnetic field strength taking into account the influence of reflections // Moscow Workshop on Electronic and Networking Technologies, MWENT 2020 – Proceedings. 2020. С. 9067494. doi: 10.1109/MWENT47943.2020.9067494
8. Шпедт Е. Р., Андреев П. Г., Гришко А. К., Наумова И. Ю. Возможности «cst studio suite» при проектировании высокочастотных устройств // Труды Международного симпозиума «Надежность и качество». 2020. Т. 2. С. 158–160.
9. Андреев П. Г., Волков В. А., Фирсова Д. И., Китаев М. Б. Возможности ANSYS HFSS при проектировании печатных плат и узлов радиоэлектронных средств // Современные информационные технологии. 2015. № 22. С. 25–28.
10. Андреев П. Г. Возможности «cst studio suite» при проектировании высокочастотных устройств // Труды Международного симпозиума «Надежность и качество». 2007. Т. 1. С. 146–148.
11. Гришко А. К., Тумакова И. А., Андреев П. Г., Мокшанцева А. В., Пакайкин А. А. Классификация естественных радиопомех и основные методы борьбы с ними // Труды Международного симпозиума «Надежность и качество». 2019. Т. 2. С. 283–287.
12. Савин М. Л., Зуев В. Д., Кочегаров И. И., Соловьева Е. М., Лысенко А. В. Методика контроля работоспособности устройства по косвенным параметрам // Надежность и качество сложных систем. 2022. № 1. С. 98–107. doi: 10.21685/2307-4205-2022-1-11
13. Куатов Б. Ж., Рыбаков И. М., Юрков Н. К. К проблеме создания цифровых моделей теплонагруженных элементов радиоэлектронной системы // Надежность и качество сложных систем. 2022. № 1. С. 9–19. doi: 10.21685/2307-4205-2022-1-2
14. Андреев П. Г., Нагаев Т. Р., Комзалова М. А. Воздействие электромагнитных импульс на радиоэлектронную аппаратуру // Современные информационные технологии. 2018. № 28. С. 48–51.
15. Гришко А. К., Андреев П. Г., Тумакова И. А., Мокшанцева А. В., Моисеев А. В., Пакайкин А. А. Применение имитационного моделирования при оценке устойчивости радиосвязи // Труды Международного симпозиума «Надежность и качество». 2020. Т. 1. С. 114–115.

References

1. L'vovich I.Ya., Voronov A.A. Application of methodological analysis in security research. *Informatsiya i bezopasnost' = Information and security*. 2011;14(3):469–470. (In Russ.)
2. Ryzhova V.A. *Proektirovanie i issledovanie kompleksnykh sistem bezopasnosti = Design and research of integrated security systems*. Saint Petersburg: NIU ITMO, 2013:156. (In Russ.)
3. Apollonskiy S.M. *Zashchita tekhnosfery ot vozdeystviya fizicheskikh noley i izlucheniy: v 3 t. T. 3. Metody zashchity ot fizicheskikh poley i izlucheniy: monografiya = Protection of the technosphere from the effects of physical zeros and radiation: in 3 vols. Volume 3. Methods of protection from physical fields and radiation: monograph*. Moscow: RUSAYNS, 2016:336. (In Russ.)
4. Andreev P.G., Yurkov N.K., Grishko A.K., Kochegarov I.I., Zhumabaeva A.S. Study of dielectric effect on signal propagation in the gigahertz range at elevated temperature. *2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF 2019)*. 2019:8840587. doi: 10.1109/WECONF.2019.8840587
5. Yurkov N.K., Andreev P., Bushmelev P. Space-time analysis of conductive paths with allowance for temperature influence. *Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM*. 2016. doi: 10.1109/SCM.2016.7519739
6. Mikheev M.Y., Roganov V.R., Andreev P.G., Goryachev N.V., Trusov V.A. Developing the structure of the quality control system of power supply units in mobile robots. *2017 International Siberian Conference on Control and Communications, SIBCON 2017 – Proceedings*. 2017:7998579. doi: 10.1109/SIBCON.2017.7998579
7. Grishko A.K., Kochegarov I.I., Lysenko A.V., Andreev P.G., Goryachev N.V., Danilova E.A. Determination of electromagnetic field strength taking into account the influence of reflections. *Moscow Workshop on Electronic and Networking Technologies, MWENT 2020 – Proceedings*. 2020:9067494. doi: 10.1109/MWENT47943.2020.9067494
8. Shpedt E.R., Andreev P.G., Grishko A.K., Naumova I.Yu. The capabilities of the «cst studio suite» in the design of high-frequency devices. *Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo» = Proceedings of the International Symposium "Reliability and Quality"*. 2020;2:158–160. (In Russ.)
9. Andreev P.G., Volkov V.A., Firsova D.I., Kitaev M.B. ANSYS HFSS capabilities in the design of printed circuit boards and electronic components. *Sovremennye informatsionnye tekhnologii = Modern information technologies*. 2015;(22):25–28. (In Russ.)
10. Andreev P.G. The capabilities of the «cst studio suite» in the design of high-frequency devices. *Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo» = Proceedings of the International Symposium "Reliability and Quality"*. 2007;1:146–148. (In Russ.)
11. Grishko A.K., Tumakova I.A., Andreev P.G., Mokshantseva A.V., Pakaykin A.A. Classification of natural radio interference and basic methods of dealing with them. *Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo» = Proceedings of the International Symposium "Reliability and Quality"*. 2019;2:283–287. (In Russ.)
12. Savin M.L., Zuev V.D., Kochegarov I.I., Solov'eva E.M., Lysenko A.V. The method of monitoring the device's operability by indirect parameters. *Nadezhnost' i kachestvo slozhnykh system = Reliability and quality of complex systems.* 2022;(1):98–107. (In Russ.). doi: 10.21685/2307-4205-2022-1-11
13. Kuatov B.Zh., Rybakov I.M., Yurkov N.K. On the problem of creating digital models of heat-loaded elements of an electronic system. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems*. 2022;(1): 9–19. (In Russ.). doi: 10.21685/2307-4205-2022-1-2
14. Andreev P.G., Nagaev T.R., Komzalova M.A. The effect of electromagnetic pulses on electronic equipment. *Sovremennye informatsionnye tekhnologii = Modern information technologies*. 2018;(28):48–51. (In Russ.)
15. Grishko A.K., Andreev P.G., Tumakova I.A., Mokshantseva A.V., Moiseev A.V., Pakaykin A.A. The use of simulation modeling in assessing the stability of radio communications. *Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo» = Proceedings of the International Symposium "Reliability and Quality"*. 2020;1:114–115. (In Russ.)

Поступила в редакцию / Received 05.08.2023

Поступила после рецензирования и доработки / Revised 10.09.2023

Принята к публикации / Accepted 25.09.2023