

УДК 369.01

Автоматизированная система управления охраной периметра протяженных территорий нефтеперерабатывающего завода АО «Куйбышевский НПЗ», трубопровода для защиты от врезок.

Медведев С.О.,

Научный руководитель д.т.н., профессор Астапов В.Н.

Самарский Государственный технический университет
Самара, Россия (443100, Самара ул. Молодогвардейская, 244), e-mail:
e-mail: stanis5232@gmail.com, asta-2009@mail.ru

Аннотация

В данной работе проведен аналитический обзор применения автоматизированных систем охраны в промышленности, образовательных учреждениях и частной собственности. Анализ данной предметной области проведен и показывает, что осуществляется защита не только самих производств, но и магистралей транспортировки сырья (трубопроводов) с применением специальных технических средств с возможной автоматизацией процесса охраны на протяженных территориях. Так же применение специальных систем на базе non-PC аналитических устройств дает возможность многократно увеличить отказоустойчивость, даже если из строя выйдет несколько элементов в данной цепи.

Ключевые слова: охранная система, безопасность, наблюдение, анализ, автоматизация, защита.

Automated control system for perimeter protection of extended territories of the Kuibyshev oil refinery jsc, pipeline for protection against tie-ins.

Medvedev S.O.,

Scientific supervisor, Doctor of Technical Sciences, Professor Astapov V.N.

Samara State Technical University
Samara, Russia (244 Molodogvardeyskaya str., Samara, 443100), e-mail:
e-mail: stanis5232@gmail.com, asta-2009@mail.ru

Annotation

In this paper, an analytical review of the use of automated security systems in industry, educational institutions and private property is carried out. The analysis of this subject area has been carried out and shows that not only the production facilities themselves are being protected, but also the highways for transporting raw materials using special technical means with possible automation of the protection process in extended territories. Thus, the use of special systems based on non-PC analytical devices makes it possible to multiply fault tolerance, even if several elements in a given circuit fail.

Key words: security system, security, surveillance, analysis, automation, protection.

Введение

В современном мире с каждым днем увеличивается количество несанкционированных проникновений злоумышленников на различные территории из-за невозможности обеспечения безопасности посредством калиточных замков и забора из различных материалов. На различных территориях, располагается крупная специальная техника и мелкая компьютерная, бытовая техника, приборы, оборудование, которая привлекает злоумышленников. Злоумышленникам зачастую удается избежать ответственности, владельцы имущества остаются в невыгодном положении. Ответственные ведомства не всегда справляются, раскрываемость преступлений по хищению имущества не велика.

В такой ситуации возникает необходимость в дополнительных средствах защиты будь то квартира, офис, предприятие и т.д., встает вопрос актуальности разработки и установки интеллектуальной системы безопасности, которая сможет в кратчайший срок оповестить владельца и соответствующие службы о проникновении. На данный момент в мире существует множество охранных систем, которые постоянно дорабатываются, модернизируются. Так же всегда есть возможность в подключении к системам умного дома и управлять удаленно.

Собственники частных территорий все чаще задумываются об установке охранного оборудования, готовы вкладывать денежные средства в разработку системы безопасности. В нынешних реалиях существует нехватка электронных компонентов.

Также существует проблема безопасности таких объектов инфраструктуры, как нефтепроводы, газопроводы и НПЗ (АО «Куйбышевский НПЗ»). Мощность данного НПЗ находится в пределах 7 млн. т. нефти в год. Специализация данного завода заключается в производстве высококачественного моторного топлива. Технологические требования к безопасности трубопроводных систем, которые были в СССР, устарели и неприменимы для современной России. У нее не только новая конституция, новые границы, но и новые угрозы энергобезопасности, новые угрозы трубопроводным системам. [1]

К особенностям охраны протяженных территорий можно отнести тот факт, что охранная система по периметру состоит из многих элементов таких как: забор, различные преграды, датчики раннего и позднего обнаружения.

Для установки таких систем, которые требуют прокладки питающих и сетевых проводов установку сенсоров и т.д. необходимы большие трудозатраты и вложения денежных средств. К каждой системе необходим индивидуальный подход из-за разности рельефа (деревьев, оврагов, водоемов). Также оказывает негативное влияние помехи, которые на протяжении всего периметра появляются в виде (искажений сигналов, затуханий). Влияние

оказывает и проходящие вблизи ЛЭП. Существует проблема ложных срабатываний датчиков. Данная проблема решается использованием распределенных кабельных сенсоров.

1 Принципы работы автоматизированной системы охраны

Это автоматизированное устройство, которое использует различные датчики, действующие на разных охраняемых территориях, управляющий модуль (контроллер) опрашивает и анализирует полученные данные на основе которых выносит вердикт об обнаружении точки проникновения на охраняемый периметр». После обнаружения контроллер отправляет уведомление владельцу о проникновении на территорию в определенном секторе. [5,7]

В основном устройство охранной сигнализации можно разделить на несколько типов:

- Охранная сигнализация, которая не имеет каналов связи с правоохранительными органами и специальными подразделениями, называется Автономной. Оповещение происходит благодаря световым и звуковым сигналам, привлекающим внимание.
- Так же существует - вид охранной сигнализации который помимо включения локальных мер оповещения (звуковым и световым) отправляет сигнал тревоги по каналам связи отвечающим ведомствам. Такая система называется системой с подключением к пульту централизованного управления.

Каналы связи бывают проводные и беспроводные. К беспроводным относятся:

- системы с GSM,
- спутниковые
- системы, построенные на радио системы передачи извещений прежде всего это, позволяет быстро и удобно организовать подключение к пульту централизованного управления.

А проводным: телефонные линии.

Важную роль в каждой охранной системе играют средства авторизации пользователя и система устройств обнаружения проникновения.

К средствам авторизации можно отнести:

- RFID метки
- NFC метки
- Системы распознавания (радужки, глаз, лица)
- Использование пароля для снятия и постановки с охраны.
- Сканер отпечатков пальцев.

- Разрешенных устройств по геолокации.

Так как помимо авторизации важную роль в системе играет сеть различных датчиков, которые предназначены для мониторинга состояния: открытия двери, целостности стекол, внутреннего объёма, движения, датчики работают посредством преобразования воздействия в электрические сигналы.

Работа таких датчиков совершенно разная и направлена на:

- Звуковые – настройка на определенные частоты;
- Измерения расстояние.
- Тепловизионные системы
- Радарные системы
- Лидарные системы
- Радио лучевые системы
- Инфракрасные системы
- Виброчувствительные системы
- Оптоволоконные
- Трибоэлектрические
- Акселерометры
- Проводноволновые системы
- Емкостные системы
- Магнитометрические системы
- Сейсмоакустические системы

Основное требование к системе безопасности заключается в скрытом монтаже средств обнаружения (СО)- размещают в почве, грунте или в другой среде. Они имеют важное тактическое преимущество: идентификация их зон обнаружения затруднена, что делает вторжение нарушителя каким-либо ухищренным способом маловероятным, при этом не допускается резкого снижения обнаружительной способности СО. Для маскируемых ПСО, как правило, источников существенных помех значительно меньше. Такие ПСО не требуют регулярного технического обслуживания, сужается диапазон предельных рабочих температур.

[6]

2 Охранный комплекс Трезор-р установленный на АО Куйбышевский НПЗ

Охранный комплекс ТРЕЗОР-Р - радиоволновое средство обнаружения (Рис. 1). Главный плюс этой системы заключается в возможности скрытой или на ограждение. Охраняемый периметр создается путем прокладывания двух высоко чувствительных кабелей, которые

могут принимать сигнал и передавать его дальше на контроллер. Сигнал генерируется в блоке ПРД и передается на провод тем самым формируется магнитное поле. При появлении постороннего объекта сигнал изменяется и подается сигнал тревоги. Принцип действия таких систем основан на анализе изменений амплитуды и фазы принимаемого сигнала, возникающих при появлении в зоне постороннего предмета. Системы применимы там, где обеспечивается прямая видимость между приемником и передатчиком, т.е. профиль поверхности должен быть достаточно ровным и в зоне охраны должны отсутствовать кусты, крупные деревья и т.п. [4]

Можно выделить следующие преимущества: не высокие показатели излучения, низкое энергопотребление, обладает высокой устойчивостью к изменениям внешних воздействующих факторов таких как (туман, ветер, птицы, вибрации, помехи от радиостанций).[2,6]

Главный недостаток таких систем заключается в наличии мертвых зон, пониженная чувствительность в районе приемника и передатчика. Что бы избежать такого эффекта необходимо устанавливать датчики с наложением 1 зоны на другую примерно 3 метра. Присутствует недостаток повышенной чувствительности на расстоянии 30-40 см над землей.

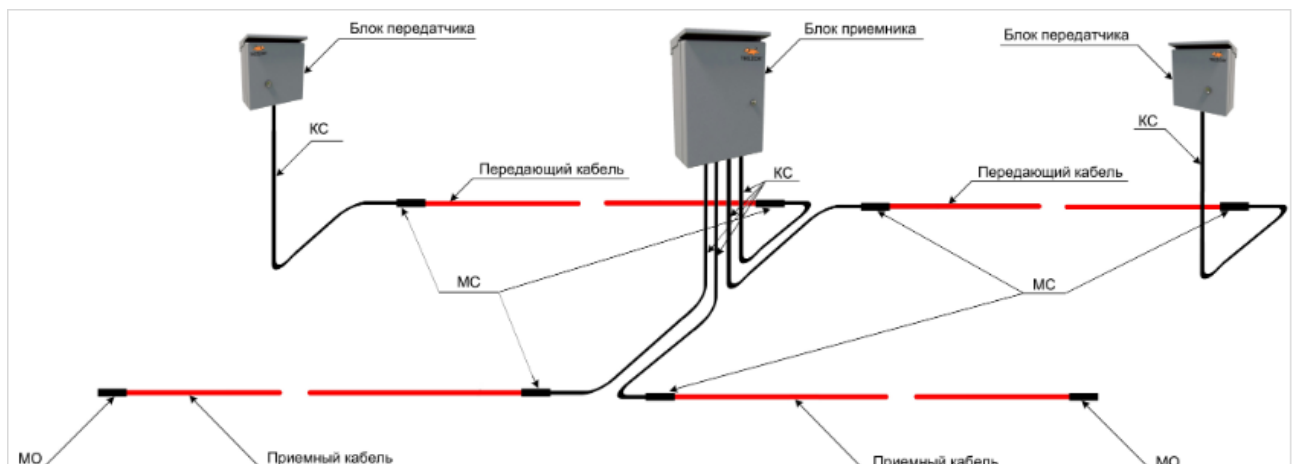


Рис. 1- ТРЕЗОР-Р

Применённые технические средства для обеспечения безопасности

(нефте-, газопровода).

Сегодня является одним из используемых методов, который позволяет в короткий срок найти место врезки путем сверления трубопровода и нейтрализовать его. Данный метод обнаруживает вибрации, которые оказываются на тело. Система построена с использованием виброакустических датчиков и управляющего контроллера. Поступающая информация с датчиков фильтруется и анализируется на присутствие аномальных помех, и в случае их

нахождения передается на экран оператора системы с указанием места и типа воздействия. Данные датчики производятся на основе пьезокерамического преобразователя и интегрируются на корпус трубопровода при помощи магнита, и заливается композитным материалом. Соединяются с контроллером при помощи специального кабеля. Промежуточные блоки связи установленные на магистрали и провода соединяющие их монтируются на специальную эстакаду. Данные блоки связи фильтруют информацию на присутствие шумов затем кодируют информацию и направляют далее на блок управления (контролер). В результате обработки сигналов рабочее ПО на ПК подтверждает или игнорирует предварительно принятую информацию магистральным блоком о наличии врезки.

Технология устроена на обнаружении микронапряжений в специальном кабеле. В его состав входит два высокочувствительных волокна, на которые подается постоянное излучение лазера. В первом контроллере излучение разделяется на два световых пучка, которые попадают в волокно. Во втором контроллере происходит интерференция обоих лучей. Если оба плеча системы находятся в невозмущенном состоянии, то интерференционная картинка на втором контроллере остается неизменной. При воздействии внешних факторов на кабель оптическая разность волокна изменяется, и второй контролер фиксирует эту разность и передает на управляющий модуль. Используемый лазер является полупроводниковым и имеет мощность (10...45) мВт, с длиной волны 1,30 или 1,54 мкм. Это позволяет увеличить расстояние контролируемой области до 55 км. Ширина покрываемой зоны составляет 6 метров.[3]

Заключение

Это связано с тем, что в этом случае злоумышленнику требуется больше времени на преодоление расстояния до цели, и, следовательно, у системы безопасности есть больше времени для действий. Однако в этом случае периметр объекта длиннее. Следовательно, увеличиваются затраты на технические средства и их эксплуатацию, а также количество необходимых сил и технических средств охраны. Поэтому при построении эффективной системы охраны объекта необходимо решить задачу оптимизации конфигурации и протяженности периметра, количества зон охраны, выбора систем охраны, физических барьеров, мер нейтрализации и отражения, а также размещения сотрудников охраны. Поэтому основной задачей при построении системы безопасности является минимизация затрат на создание и эксплуатацию системы безопасности и содержание персонала охраны при заданном эффекте защиты и существующих характеристиках периметра (конфигурация, длина). Для многих предприятий актуальна проблема краж ценностей. Очевидно, что лучшим

способом решения этой проблемы является увеличение высоты ограждения или увеличение расстояния от внутренней части до барьера, но это не всегда возможно. Во многих случаях целесообразнее использовать периметральные системы охраны, которые располагаются с внутренней стороны ограждения или крепятся на объект охраны нефтепровод и имеют наибольшее расстояние от забора. Это объясняется тем, что порядок работы, установленных на разных периметрах, позволяет службе безопасности определить направление движения злоумышленников. Дополнительным аргументом в пользу решения об организации охраны периметра является то, что она является неотъемлемой частью общей системы, без которой невозможно организовать эффективную систему доступа на предприятие. Наличие такой охраны полностью гарантирует, что сотрудники могут входить и выходить из компании только через регламентированные точки доступа. Важным фактором, сдерживающим создание систем охраны периметра объектов, является их относительно высокая стоимость. Из соображений экономической целесообразности принято считать, что охрана периметра охраняемого объекта необходима, если ее стоимость не превышает 10% от стоимости активов охраняемого объекта.

Список литературы

1. ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования. – Москва: Стандартинформ, 2010.
2. ГОСТ Р 52651-2006. Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2007. – 19 с.
3. ГОСТ Р 52435-2015. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2016. – 28 с.
4. Охранная сигнализация трубопроводов [Электронный ресурс] Эл. Ресурс http://secuteck.ru/articles2/prof_dialog/zaschita-truboprovodov-ot-vrezok.
5. Р 78.36.005-99 Рекомендации. Выбор и применение систем контроля и управления доступом. - М.: МВД РФ, НИЦ «Охрана» ГУВО. 31 марта 1998.
6. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Проектирование технических средств защиты территорий и объектов от несанкционированного доступа : учеб. пособие / А. В. Тельный ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2020. – 251 с.
7. Волковицкий В.Д., Волхонский В.В. Цифровые системы ТВ-наблюдения // БДИ. Безопасность, достоверность, информация. СПб., 2009. № 5. С. 38-47.