Форум Технологии Безопасности онлайн конференция 18.05.22

Тема конференции: «Комплексная безопасность и защищенность объектов промышленности, нефтегазового сектора и электроэнергетики»

Докладчик ООО «Охранная техника»

Тема доклада: «Интеграция периметральных средств охраны в комплексную систему охраны».



Добрый день коллеги.



Многие уже строят системы «УМНОГО ДОМА», а что у нас с «УМНЫМИ ПРЕДПРИЯТИЯМИ»?

Недостаточно обнаружить нарушителя, необходимо обеспечить бесперебойную работу системы охраны, взаимодействие составляющих частей.

Всё это можно реализовать в интегрированном комплексе технических средств охраны.

Интегрированные системы позволяют оперативно реагировать на несанкционированное проникновение, включать другие системы реагирования и локализации, вести мониторинг работоспособности, удалённо управлять и подстраивать систему.



Какие возможности даёт комплексная система охраны?

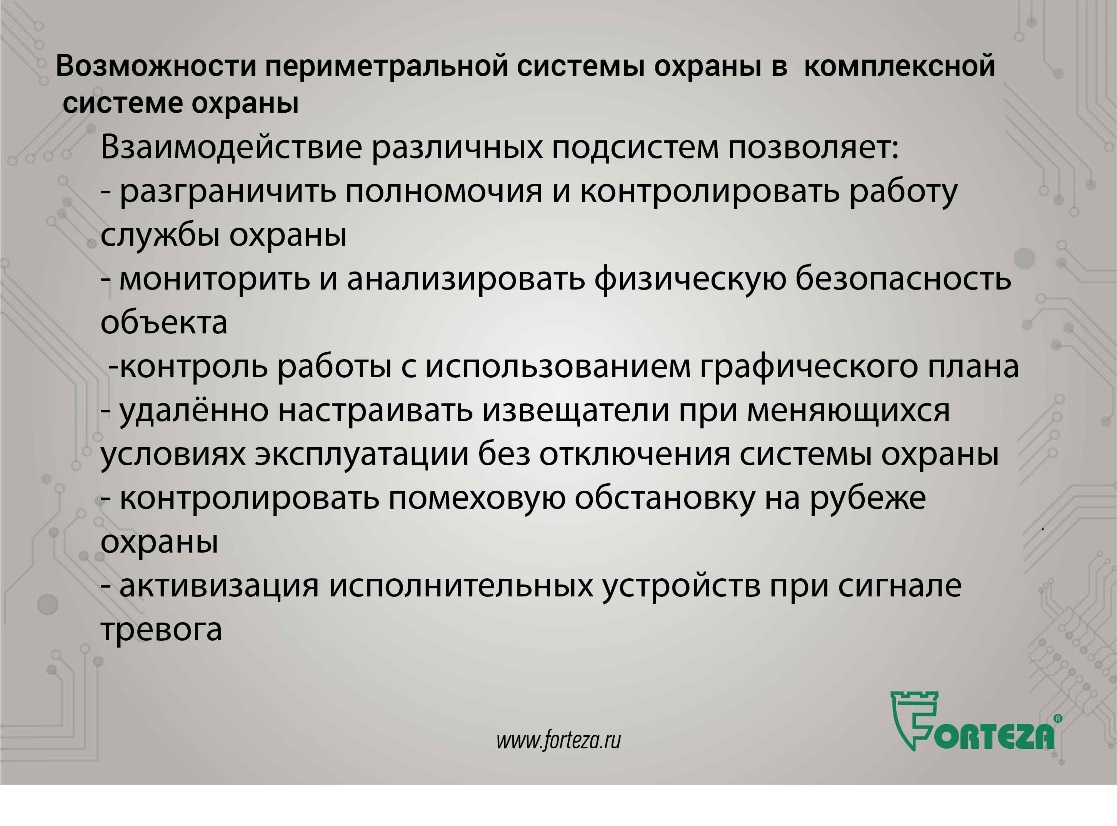
- увеличение надёжности защиты объекта за счёт взаимодействия различных систем охраны

- контроль исполнения организационных мероприятий (по обеспечению контрольно-пропускного режима; действий службы физической охраны при поступлении тревожных сообщений и несении службы; периодичности проведения технологических и регламентных работ на оборудовании ТСО и др.)

- облегчить работу обслуживающего персонала за счет автоматизации процессов управления, контроля и принятия решений по обеспечению безопасности

- снизить затраты на монтаж и эксплуатацию системы безопасности, сокращение обслуживающего персонала и затрат на его обучение и содержание

Возможности периметральной системы охраны в КТСО для обеспечения взаимосвязи подсистем:



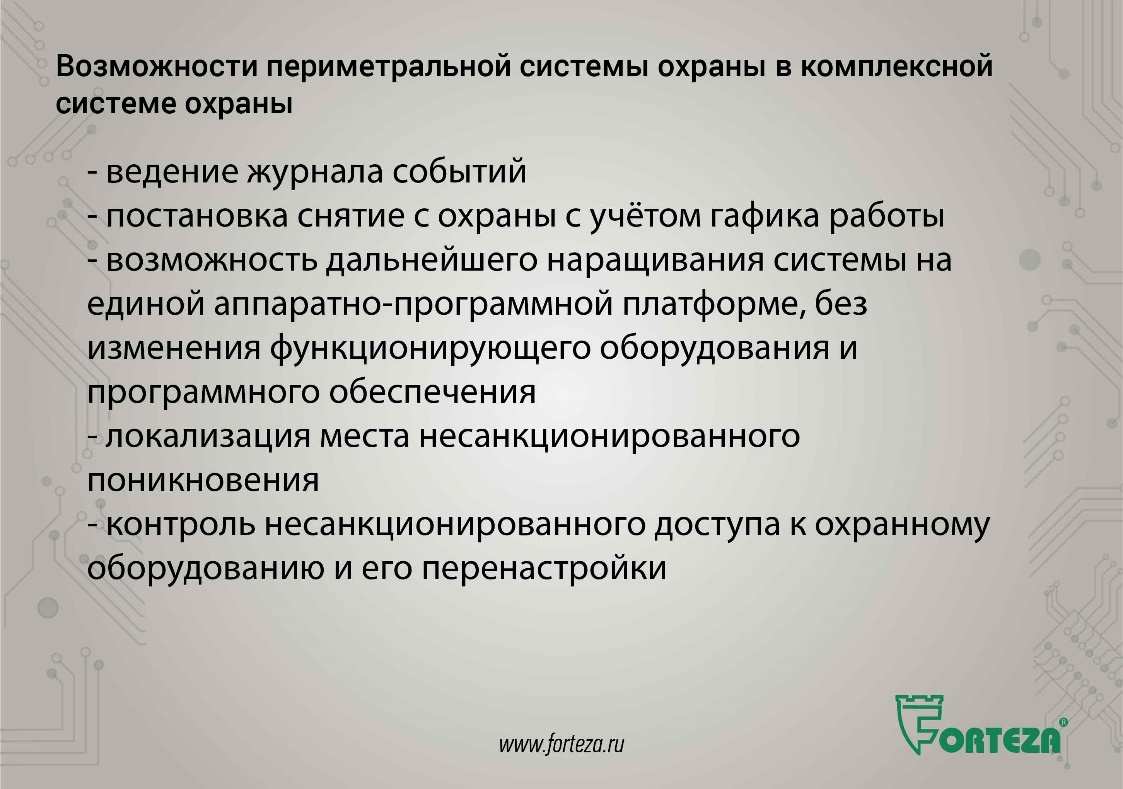
Взаимодействие различных подсистем позволяет:

- мониторить и анализировать физическую безопасность объекта с учётом разграничения полномочий и контроля работы службы охраны;

- наглядно видеть работу системы охраны на графическом плане объекта;

- контролировать помеховую обстановку на рубеже охраны и при необходимости удалённо настраивать извещатели при меняющихся условиях эксплуатации без отключения системы охраны;

- активизация исполнительных устройств других подсистем при срабатывании сигнала тревога.



Часть этих функций обязательна, другая желательна, некоторые не обязательны в зависимости от требований к охраняемому объекту. ГОСТ Р 57674-2017 определяет структуру основных (обязательных) подсистем информационных систем безопасности (ИСБ).

При грамотном построении комплексной системы охраны можно минимизировать влияние человеческого фактора на надёжность системы охраны.

Правда давайте вспомним доклад на конференции Форума Технологии Безопасности представителя службы охраны Крымского моста. Установленная система позволяет максимально автоматизировать работу, но было принято решение реагировать и проверять все инциденты. Для такого объекта это грамотное решение, но интегрированная комплексная система охраны, всё равно, облегчает работу служб, и повышает её надёжность за счёт более полной анализируемой информации.

Модель работы выбирать потребителю в зависимости от условий объекта, возможных последствий от несанкционированного проникновения.



Перейдём к видам интеграции:

- Аппаратная: когда периферийное оборудование по сухим контактам реле через адаптеры (контроллеры) подключаются к системе охраны. Преимущество – можно подключить любое периферийное оборудование по сухим контактам реле. Недостаток - система имеет ограниченный функционал из-за отсутствия канала обратной связи и ограниченного количества информации о периферийных устройствах, анализируемых системой. Кроме того, требует прокладки пары проводов к каждому извещателю. Это значительное удорожание при устройстве системы.

- Программная: периферийное оборудование, например по интерфейсу RS-485, подключается к системе охраны. Система позволяет расширить функционал и значительно сократить стоимость сети связи. Используется одна витая пара на шлейф сигнализации, по которой происходит управление периферийными средствами обнаружения и исполнительными устройствами.

В настоящее время почти все подсистемы безопасности имеют возможность программного управления с помощью АРМ на персональном компьютере, но, к сожалению, второй вид интеграции не всегда возможен при использовании оборудования разных производителей, из-за нежелания производителей использовать открытые протоколы обмена или прописывать стороннее оборудование в своих системах.

Пример программной интеграции:

- интегрированная система безопасности Intellect от ООО "Ай Ти Ви Групп";

- программа Орион-Про от компании Болид с пультом С2000М

- Аппаратно-программная: совмещающая принципы двух предыдущих. Высокая функциональность и выше надежность системы, так как в случае выхода из строя компьютера управления или сбоя в работе ПО интеграция сохраняется.

Например, аппаратно-программная интеграция широко используется при использовании извещателей, требующих оперативной настройки при изменении условий эксплуатации (сезонная настройка).

Рассмотрим подключение трибоэлектрического извещателя ЛИАНА производства ООО «Охранная техника».

Хотя чувствительный элемент извещателя ЛИАНА и мало меняет свои обнаружительные свойства при понижении температуры (в несколько раз по сравнению с чувствительными элементами из коаксиального кабеля) и кроме того, имеет систему термокомпенсации, всё равно надо отслеживать уровень шума и учитывать его.

Архитектура подключения простая и эффективная. Извещатель для передачи тревожного извещения подключается через адаптер по сухим контактам реле, а для мониторинга и настройки используется интерфейс RS-485. В этом случае не требуется интеграция программы настройки в комплексную систему охраны и можно удалённо корректировать обнаружительную способность извещателей без отключения периметра от системы охраны. И при корректировке можно обойтись без использования на открытом воздухе оборудования настройки, имеющего ограничения использования при низких температурах.

Тем более такая архитектура интересна, так как некоторые разработчики комплексных систем охраны не охотно идут на включение программ настройки в свои программные продукты.

Аналогично можно подключить двухпозиционные радиоволновые извещатели серий ФОРТЕЗА, ФОРТЕЗА-М, КУПОЛ-20.; однопозиционные радиоволновые извещатели серий ЗЕБРА (работающих на частотах 5,8; 9 и 24 ГГц); и другие извещатели торговой марки Forteza.

Пример аппаратно-программной интеграции:

- программа Орион-Про от компании Болид с пультом С2000М;

- система Рубеж компании Сигма-ИС.

В эти системы интегрированы и извещатели торговой марки Forteza.

По принципу построения системы являются совокупностью адресных, распределённых аппаратно-программных элементов, образующих иерархическую, модульную, распределенную аппаратно-программную структуру. Недостаток этих систем – работа только с периферийным оборудованием, прописанным в программу разработчиком. Остальное оборудование можно использовать путём подключения по сухим контактам через адаптер, при этом ограничивается функционал. Сегодня это недостаток большинства систем с аппаратно-программной интеграцией. Но описанная выше схема позволяет расширить функционал.



Для создания программной интеграции в систему охраны необходимо выполнять некоторые условия требования к системе передачи данных:

- Протокол обмена данными между командами комплексной системой охраны и периферийным оборудованием.

И здесь опять актуален вопрос создание единого протокола. Что бы при модернизации извещателей или создании новых извещателей система распознавала тип оборудования и понимала команды, посылаемые и принимаемыми периферийными устройствами, без внесения дополнительных изменений в программные продукты.

Протокол обмена данными можно вшить как в саму программную оболочку системы охраны, так и адаптеры, посредством которых происходит подключение в систему охраны, или непосредственно в извещатели.

Адаптеры удобнее если интегрированы извещатели разных производителей.

Надо учитывать, что накладываются ограничения по длине интерфейсной линии RS-485 в 1 200 м. Но его можно обойти, используя репитеры для ликвидации искажения затухающего сигнала (ещё называют: усилители сигнала, повторители интерфейса). Репитеры позволяют увеличить длину линии до 3 600 м.



Почему разработчики комплексных систем охраны не идут на использование автоматической программной интеграции, работой по принципу Plug and Play (включай и работай)?

Причин много, и как уже обсуждалось на площадке ТБ Форума, это конкурентные преимущества производителей систем охраны при закрытых протоколах обмена.

Хотя нам кажется это сложившаяся практика. К началу внедрения стандартных открытых протоколов обмена основные производители уже использовали свои закрытые протоколы.

Переходить на новые стандартные открытые протоколы требует затрат. А при закрытых протоколах трудоёмко без конца обновлять свои программы в связи с изменением линейки периферийных устройств. Тем более затратно включать в свои программы блоки для удалённой настройки.

Это становиться понятно если рассмотреть подходы, которые используют разработчики оборудования и программного обеспечения для создания комплексной технической системы охраны:

1 - Создание под платформу своего программного обеспечения Информационной Системы Безопасности (ПО ИСБ) программных драйверов для возможности подключения оборудования других производителей (например, ПО „Интеллект“ фирмы ITV). Такой вариант возможен как по соглашению между разработчиками программной платформы и оборудования ИСБ, так и без соглашения со вскрытием протоколов по инициативе заказчика или монтажной организации при проведении пусконаладочных работ на объекте.

2 - Использование контроллеров, запрограммированных производителем по соглашению между разработчиками.

3 - Использование программируемых промышленных контроллеров или преобразователей интерфейсов различных производителей, которые программируются заказчиком или монтажной организацией при проведении пусконаладочных работ на объекте.

И подходы с открытыми протоколами обмена:

4 - Разработчики ПО ИСБ выпускают платформы с открытой архитектурой для того, чтобы пользователи могли самостоятельно в АРМ ИСБ обмениваться с ИСБ других производителей (например, на основе протокола ModBus (основан на архитектуре ведущий-ведомый)).

5 - Разработчики линейки ИСБ создают для своего оборудования программируемые модули и OPC-серверы, предоставляют протоколы ModBus или используют протоколы стандарта LONWORKS (локальная оперативная сеть) с промышленно выпускаемыми контроллерами. Такой подход позволяет полнофункционально интегрировать различные ИСБ на основе **SCADA**-платформ (**SCADA** аббревиатура от английскогоSupervisory Control And Data Acquisition — диспетчерское управление и сбор данных).

6 - Разработчики ИСБ интегрируют свои продукты на основе менее распространенных и более закрытых информационных технологий с использованием **SCADA**-платформ.

Опираясь на анализ экспертов (Юрий Михайлович Монахов доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации), наиболее перспективным представляется интеграция на основе **SCADA**-платформ с использованием контроллеров и серверов.

В том числе, потому что при обновлении линейки периферийного оборудования разработчику ИСБ приходится заново программировать контроллеры, что для заказчика экономически невыгодно. В то же время обновление драйверов от разработчика периферийного оборудования осуществляется, как правило, в порядке технической поддержки.

На отечественном рынке производителей оборудования и АРМ ИСБ в настоящее время кто то использует SCADA-платформы, другие интегрируются в системы на основе SCADA-платформы.

Принцип построения работы комплексной системы охраны через БИБЛИОТЕКУ данных, широко используемый в зарубежных аналогах. Когда разработчик ПО включает в свой продукт блоки, разработанные производителями периферийных устройств. В России такая работа почти не ведётся.



Для небольших объектов использование сложных программных комплексов является избыточным. Поэтому разрабатываются более простые программные системы по аналогии с УМНЫМ ДОМОМ.

Нужны и простые системы и сложные, выбирать потребителю.

На фоне различных подходов наше предприятие решило создать надёжный и удобный в пользовании программный продукт – системы сбора информации ФОРТЕЗА-ПЕРИМЕТР. Программа предоставляется бесплатно и дорабатывается по пожеланиям потребителя.

Программное обеспечение ФОРТЕЗА-ПЕРИМЕТР первоначально создавалась для проверки работоспособности оборудования торговой марки Forteza во время пусконаладочных работ.

Сегодня программа ФОРТЕЗА-ПЕРИМЕТР предназначена для контроля и управления охранными извещателями периметра торговой марки Forteza, имеющими интерфейс RS-485, а также других извещателей с НЗ-контактами, подключенными через адаптер внешних устройств ФОРТ-А. Количество линий – 4, количество устройств на линии – 32, максимальное количество устройств – 128.

ПО "ФОРТЕЗА-ПЕРИМЕТР" имеет интуитивно-понятный дружественный интерфейс, работа с которым не требует специальной подготовки.



На сегодня программой выполняются следующие функции:

- Графическое отображение устройств на карте. в качестве графического плана используется любой графический файл (спутниковая карта, схема, чертёж объекта в формате JPG, PNG, BMP). Мышкой просто расставляются, обнаруженные программой, извещатели на изображение объекта.

- Автоматический поиск подключенных устройств (не надо прописывать устройства, информация появляется автоматически).

- Контроль подключенных извещателей и цветовая индикация их состояния: постановка/снятие с охраны извещателей, тревога, норма, неисправность, с отображением на графическом плане. Дистанционный контроль реализован как сигнал неисправности при потере связи.

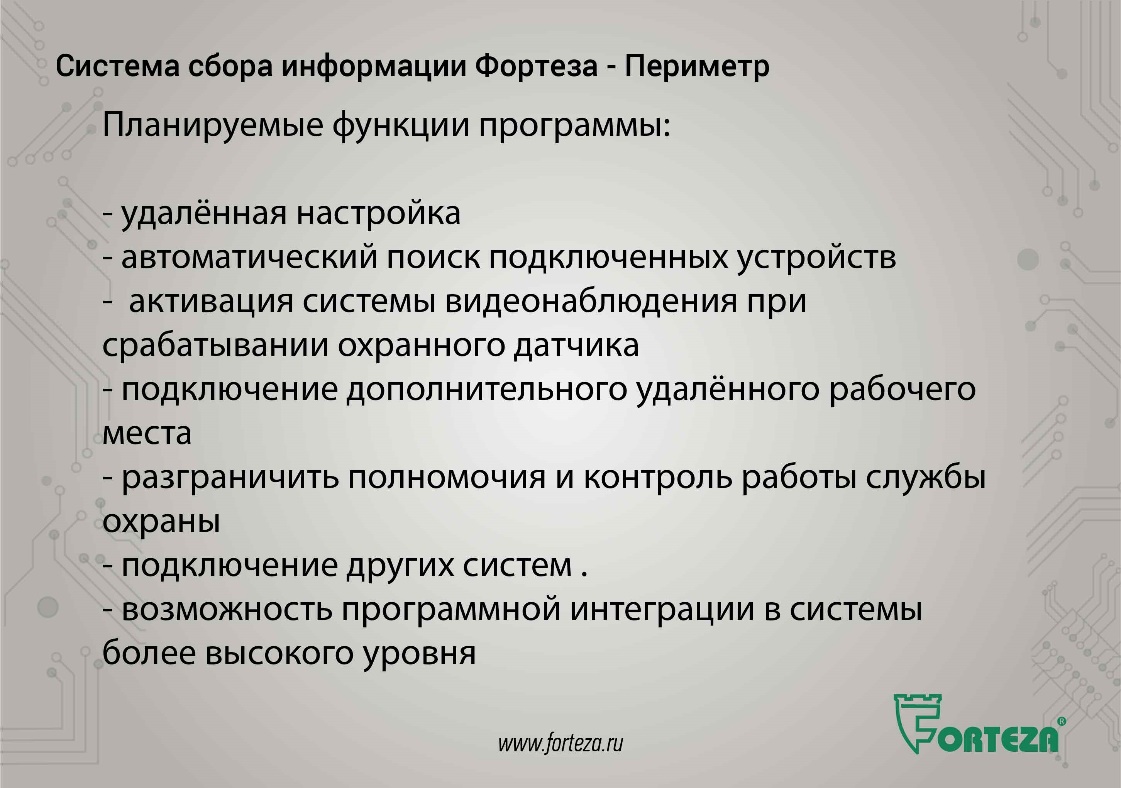
- Ведение протокола событий, поиск события по заданному фильтру и печать протокола.

- Управление исполнительными устройствами (срабатывание датчика активирует системы освещения, оповещения). Управление яркостью прожекторов охранного освещения ФОСФОР (по сценарию или ручное).

- Локализация места несанкционированного проникновения для некоторых типов извещателей.

- Контроль несанкционированного доступа к охранному оборудованию.

- Комплексное предоставление информации оперативному дежурному и ответственным лицам.



Планируется:

- Удалённая настройка извещателей при меняющихся условиях эксплуатации без отключения системы охраны.

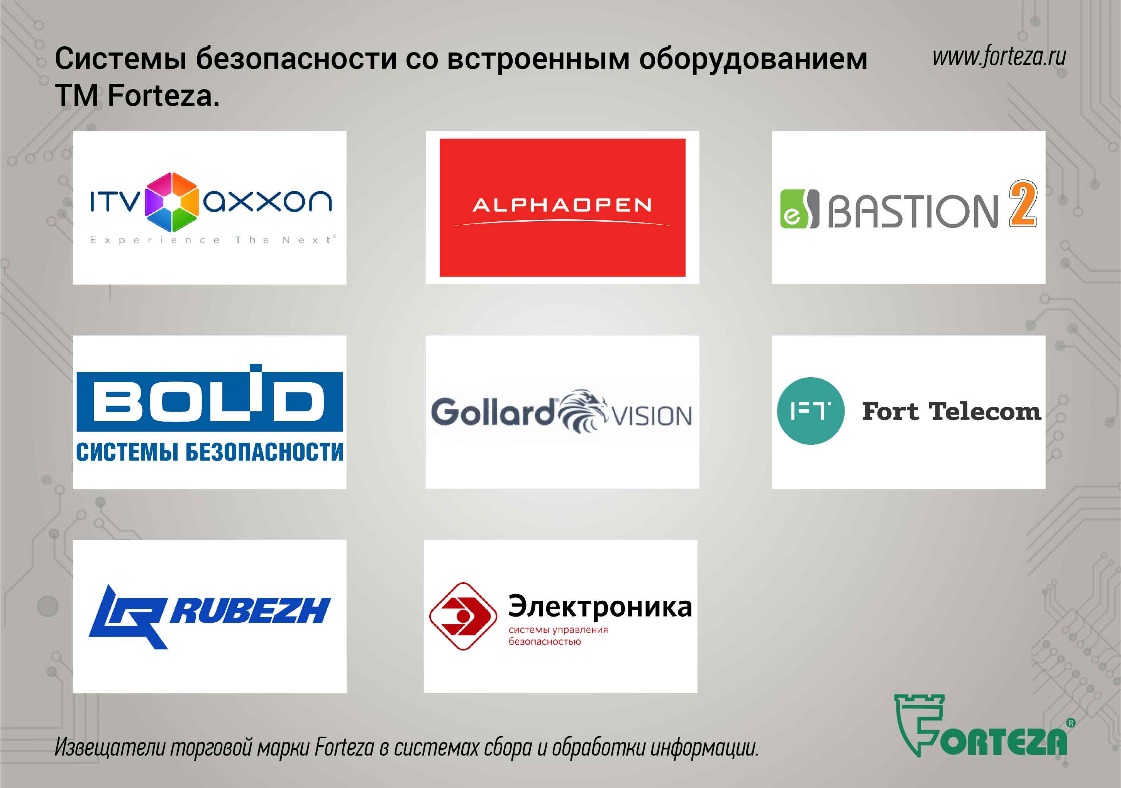
- Активация системы видеонаблюдения при срабатывании охранного датчика.

- Подключение дополнительного удалённого рабочего места.

- Разграничить полномочия и контроль работы службы охраны.

- Подключение других систем охраны.

- Возможность программной интеграции в системы более высокого уровня.



Извещатели торговой марки Forteza интегрированны в наиболее распространённые интегрированные системы охраны:

АРМ Орион Про – программно-аппаратная интеграция;

ИСБ Intellect – программная интеграция;

программная платформа Alphalogic;

Система управления безопасностью Electronika Security Manager (ESM).

Так же наши извещатели интегрированы в КТСО ПОСТ 1СВ; АПК Бастион-2; Рубеж.

Естественно, не могу не вспомнить разработчика цифровых интеллектуальных интегрированных систем безопасности Консорциум ИНТЕГРА-С, который участвует в сегодняшней конференции.



В данные системы охраны интегрированы практически все извещатели торговой марки Forteza.

Вам хорошо известны:

- двухпозиционные радиоволновые извещатели серий ФОРТЕЗА, ФОРТЕЗА-М;

- однопозиционные извещатели серий ЗЕБРА;

- комбинированные извещатели серий ФОРМАТ и ЦИКЛОП;

- проводноволновые извещатели РЕЛЬЕФ;

- вибрационные извещатели ЛИАНА и ЛИАНА-Универсал;

- охранные прожектора серии ФОСФОР.

Документацию, подробную информацию, видеозаписи учебных материалов Вы можете посмотреть на нашем сайте FORTEZA.ru.



На этом доклад заканчиваю, спасибо за внимание, готовы ответить на Ваши Вопросы.