Охрана периметра

Эффективная охрана периметра способна предотвратить несанкционированные посягательства на материальные и нематериальные ценности предприятия.

«Центр речевых технологий» предлагает комплексное решение для повышения эффективности системы охраны периметра на базе своих уникальных разработок в области аудио- и видеонаблюдения, автоматического оповещения по различным каналам связи и передовых достижений в области синтеза, распознавания речи и голосовой биометрии.

Зачем нужна охрана периметра?

Не секрет, что охрана периметра является одним из наиболее распространенных инструментов снятия головной боли за сохранность своего имущества как среди частных лиц, так и среди бизнес-сообщества. Периметр охраняемого объекта – это первое, с чем столкнется злоумышленник при попытке осуществить несанкционированное проникновение.

Экономическая целесообразность построения системы охраны периметра напрямую связана с величиной потенциального ущерба, который могут нанести «нежелательные гости» в результате незаконного проникновения. Поэтому стоимость решений для охраны периметра не должна выходить за рамки «разумного».

Каковы факторы интенсивности утечек?

Чтобы построить эффективный охраняемый периметр, необходимо учесть несколько критически важных факторов:

1. Периметр должен быть сплошным – бесполезно тратить деньги на систему безопасности, которую можно просто обойти.

2. Система охраны периметра должна не только фиксировать факт несанкционированного проникновения, но и наглядно его подтверждать.

3. Система обнаружения проникновения должна уметь оповещать ответственных лиц согласно установленному регламенту.

4. Система охраны должна иметь комплекс эффективного определения «свой-чужой» в рамках системы контроля и управления доступом для сокращения уровня ложных срабатываний на периметре и внутренних рубежах и создания комфортных условий для лиц, имеющих право свободного доступа к охраняемому объекту.

Как создать эффективную систему охраны периметра?

Эффективная система охраны периметра должна содержать сплошное наблюдение за периметром, инструменты подтверждения проникновения, комплекс тревожного оповещения по различным каналам связи, а также эффективную систему контроля и управления доступом, чтобы не превращать охраняемый объект в тюрьму для его вполне легальных обитателей.

Опыт «Центра речевых технологий» в области видеонаблюдения, организации экстренного оповещения по различным каналам связи, а также применения технологий голосовой биометрии для разграничения доступа позволяют решить эти задачи.

1. Внедрите сплошное видеонаблюдение

2. Внедрите комплекс оповещения по различным каналам связи

3. Внедрите систему голосовой биометрической верификации в качестве СКУД

Инструмент 1: Внедрите сплошное видеонаблюдение за периметром

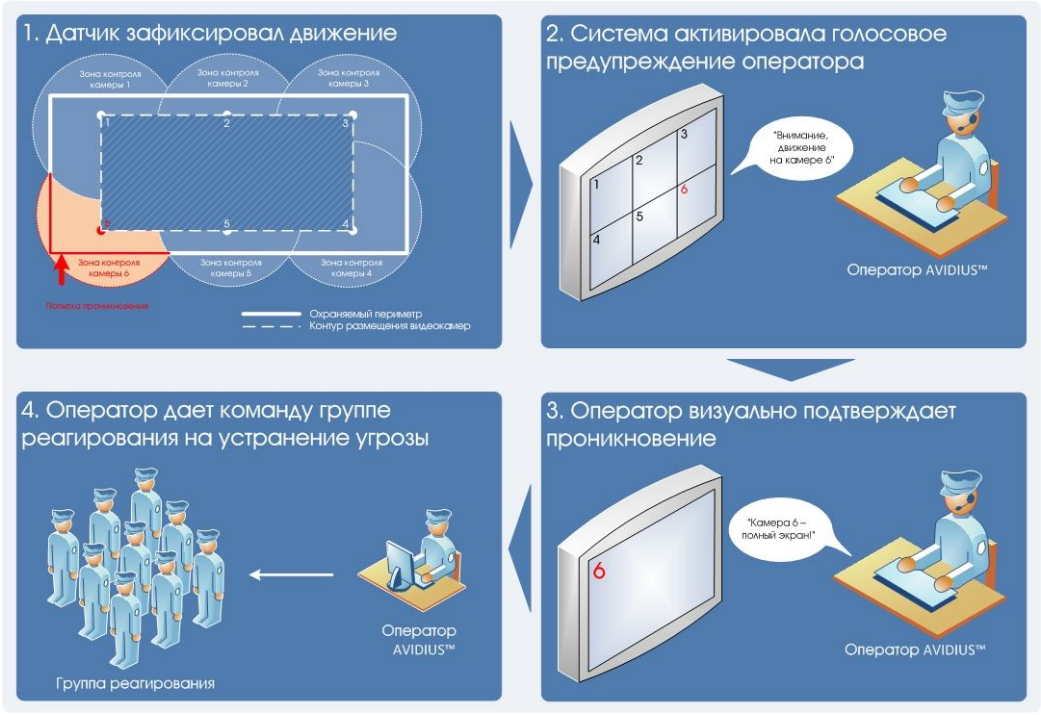
Особенность системы видеонаблюдения заключается в том, что она способна выступать как в роли системы обнаружения нарушения периметра, так и в роли системы подтверждения. Использование системы видеонаблюдения AVIDIUS™ способно успешно решить обе эти задачи.

К примеру, в случае нарушения периметра в том месте, где «свои» не ходят, система способна детектировать движение, тем самым привлечь внимание к обнаружению «чужого». С другой стороны, комплекс видеонаблюдения можно оснастить дополнительными внешними датчиками, чтобы оператор в нужный момент получал необходимое изображение на мониторе, служащее основанием для принятия решения.

Критически важным для успешного обнаружения и подтверждения несанкционированного проникновения является возможность управления поворотом камер, расположенных по периметру и на внутренних рубежах охраны. Этот функционал позволяет расширить угол обзора и уменьшить общее количество камер в системе, что сокращает стоимость всего решения.

Отличительным свойством систем видеонаблюдения, предназначенным для создания действительно эффективных комплексов охраны периметра, является возможность записи звука. Аудиозапись расширяет возможности систем мониторинга нарушения периметра особенно в темное время суток, когда злоумышленники пытаются воспользоваться плохой видимостью для несанкционированного проникновения. В то же время звукозапись переговоров может служить в качестве профилактического средства в случае, когда удается детектировать подозрительные разговоры в радиусе действия видеокамер.

AVIDIUS™ позволяет эффективно обеспечивать охрану периметра >



К тому же, необходим удобный интерфейс для управления множеством камер. Скорость и удобство переключения между камерами, управления их движением, приближения изображения и многих других функций – все это определяет скорость реагирования охраны на нарушение. Поэтому идеальным для системы видеонаблюдения является голосовое управление, позволяющее мгновенно произносить последовательность команд, ускоряющих работу оператора.

Для любого средства обнаружения правонарушения критически важным является возможность привлечения внимания оператора к движению в поле зрения установленной камеры. Фраза «Движение на камере 1» в этом плане является наиболее эффективным средством, к тому же она подсознательно стимулирует оператора к произнесению голосовой команды «Камера 1 – полный экран». Таким образом, сокращается общее время реакции охраны на тревогу.

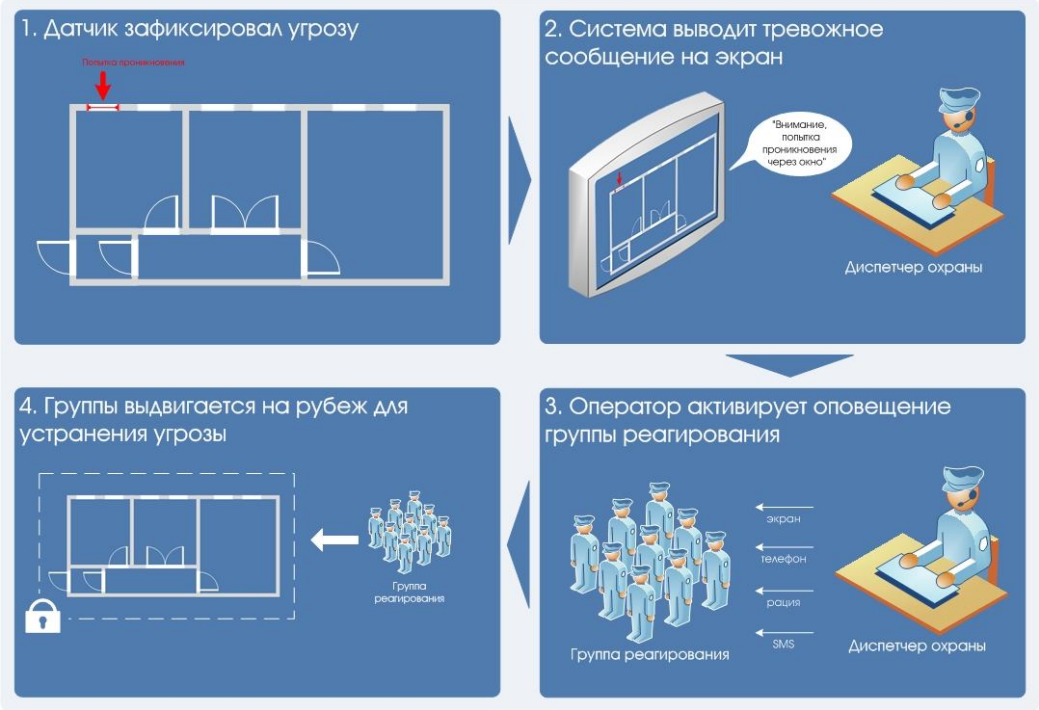
Сочетание передовых технологий в области видео- и аудиозаписи и речевых технологий в одной системе AVIDIUS™ позволяют значительно повысить эффективность видеонаблюдения в качестве обязательного компонента эффективной системы охраны периметра.

Инструмент 2: Внедрите комплекс оповещения ответственных лиц по различным каналам связи

Следующим этапом после обнаружения и подтверждения факта правонарушения для эффективной системы охраны периметра является реагирование на него. И здесь возможен широкий спектр подходов. Функционал системы автоматического оповещения Рупор™ объединяет их в одном едином комплексе.

Если объект имеет стратегическую важность, то группа реагирования, как правило, находится внутри периметра и имеет возможность достаточно оперативно выдвинуться на рубеж и пресечь

Рупор™ - высокоэффективный инструмент для нивелирования угроз >



несанкционированное проникновение. Однако для множества охраняемых зданий и сооружений бывает достаточным наличие одной группы реагирования на несколько объектов. При этом ключевым моментом является скорость реагирования, которая напрямую зависит от эффективности системы оповещения охраны.

Оповещение охраны будет более эффективным, если оно осуществляется по различным каналам связи. Так, например, целесообразно одновременно оповещать и диспетчера группы охраны, и саму группу, оставив на совести диспетчера лишь подтверждение выезда группы и контроль. В результате сокращается количество передаточных звеньев, увеличивающих интервал между поступлением тревожного сигнала и выездом группы. При этом гибкость системы оповещения должна позволять использовать любые организационные решения в области оповещения (например, оповещение диспетчера – на монитор и по стационарной телефонной связи, а оповещение руководителей групп реагирования – через SMS или по рации). Это позволяет, с одной стороны, сохранить координирующую роль диспетчера охраны, а с другой – поддерживать постоянную готовность и мобильность групп реагирования.

Не менее важным фактором эффективного оповещения является способ формирования тревожного сообщения. Ведь разные каналы связи используют различные сигналы и воздействуют на ответственные за их прием органы чувств, а скорость распознавания сигнала критически важна для сферы безопасности. Поэтому оповещение на экран должно демонстрировать графически, на каком участке рубежа возникла угроза. Тревожный звонок на стационарный или мобильный телефон, а также сообщение по рации должны содержать точную и обстоятельную информацию, причем внятно и доходчиво произнесенную, SMS-сообщение также должно быть кратким и максимально

емким, адекватно характеризующее уровень тревоги и локализацию угрозы. По этой причине, конфигуратор сообщений и способ их распространения имеет такую важность. Для формирования сообщений по телефону оптимально использование технологии синтеза речи, которая создает высокую степень гибкости для администратора системы. С применением синтеза речи отпадает возможность записывать сообщения с помощью микрофона для каждого варианта тревожного сообщения. Достаточно настроить удобный конфигуратор текстовых сообщений и активировать автоматическое синтезирование речи.

Комплекс автоматического оповещения Рупор™ сочетает в себе уникальные достижения в области речевых технологий и современных систем связи и передачи данных для формирования эффективной системы охраны периметра.

Инструмент 3: Внедрите систему голосовой биометрической верификации в качестве СКУД

Охрана периметра не всегда осуществляется в ночное время суток, когда на объекте нет посторонних. Эта задача может быть поставлена и для обычного рабочего дня, когда охраняемый объект полон сотрудников и посетителей, имеющих право на нем находится согласно трудовому или иному распорядку. Таким образом, встает сложная задача по реализации прав доступа на объект для «своих» и охрана от проникновения «чужих». Одним из наиболее эффективных средств управления и контроля доступом является голосовая биометрическая верификация на базе технологии VoiceKey™.

Преимущества голосовой биометрической верификации лежат прежде всего в области объекта верификации. Если в RFID и аналогичных системах, где объектом для сравнения с эталоном служат карточки, номера, пароли и т.д., СКУД определяет «своего» по наличию у него неких предметов или его знаний, то в биометрической системе проверяется сам человек и его неотъемлемые признаки.

Преимуществом голоса над другими признаками служит его «бесконтактность» и «физическая неотделимость» от владельца. Отсутствие контакта предпочтительно прежде всего из «гигиенических» соображений, поскольку использование отпечатка пальца или прислонение к фиксатору лица для сканирования радужной оболочки или сетчатки глаза в общественном месте может вызывать дискомфорт у персонала охраняемого объекта. Неотделимость голоса техническими или какими-то иными средствами связана с тем, что на сегодняшний день компактная техника не способна воспроизводить звук такого уровня качества, при котором считываемые системой верификации признаки совпадали бы с оригиналом без технических искажений.

Физическая реализация СКУД на базе технологии голосовой биометрической верификации включает в себя наличие электронных замков, открываемых в результате успешной верификации с помощью микрофона, находящегося рядом с необходимой дверью и подключенной по локальной сети к серверу верификации. Возможно и создание автономного голосового замка, однако это потребует от администратора отдельного обучения системы для каждой такой двери. Но поскольку автономность зачастую необходима для помещений с крайне ограниченным доступом, то и количество таких замков достаточно незначительно, а следовательно, и обучение не вызовет трудностей.

Технология голосовой биометрической верификации VoiceKey™ способна значительно укрепить охрану объекта в будние дни и в рабочее время, когда интенсивность допускаемых к объекту посетителей значительно осложняет работу службе охраны. Голосовая биометрическая СКУД является мощным инструментом обеспечения безопасности охраняемого объекта.

Контакты

Санкт-Петербург

196084
ул. Красуцкого, 4
Тел. +7(812) 325-8848
Факс: +7(812) 327-9297
info@speechpro.ru

Москва

101000
Армянский пер., 7
Тел. +7(495) 623-5505
+7(495) 623-4742
+7(495) 623-3437
stc-msk@speechpro.com

Центр речевых технологий
http://speechpro.ru/