СИГНАЛИЗАЦИЯ — БЫЛА, ЕСТЬ И БУДЕТ

АРТЕМ СИДОРОВ,
эксперт охранной организации «Аксиома Безопасности»
ohrana@aksioma-gkb.ru

В статье прослеживается история развития сигнализации — от древнейших способов защиты частной собственности до современных охранных возможностей. Рассматриваются научные и технические достижения, повлиявшие на эффективность и популярность охранных систем, а также альтернативный способ защиты территории и имущества от посторонних — системы контроля доступа. Приведена краткая история модернизации СКУД, описаны возможности применения биометрии.

ИСТОРИЯ РАЗВИТИЯ ОХРАННОЙ СИГНАЛИЗАЦИИ

Необходимость охраны материальных ценностей появилась еще в древние времена вместе с возникновением понятия «частная собственность» после распада общинного строя. Стремление защитить свое имущество от разрушений и разграблений существует у людей на уровне инстинкта. Охранная сигнализация имеет довольно длинную и весьма интересную историю. Так, например, еще в Древнем Египте фараоны стремились оградить свои усыпальницы от хищений с помощью различных ловушек — падения каменных глыб или обрушивающихся тонн песка, которые вели к гибели злоумышленников. Все это, и даже более того, нашло отражение в современных компьютерных играх жанра Quest/Adventure.

Вычислить приближение нежелательных гостей людям прежде всего помогали животные и птицы. Так, например, всем известна легенда о том, как гуси спасли Рим. Согласно ей, галлы попытались захватить римскую крепость ночью, когда защитники крепости спали. Гуси же, жившие при храме в крепости, громко загоготали, разбудив воинов и предотвратив, тем самым, вторжение в крепость.

А в средневековой Японии для защиты замка было сконструировано напольное покрытие «Угуису бари», издававшее звуки, похожие на пение разных птиц. В переводе с японского такое изобретение называется «соловьиный пол», главной целью которого являлась защита от врагов. С внутренней стороны брусьев, к которым крепились половые доски, гвоздями прикреплялись металлические пластины, издававшие при давлении на них сверху звуки, похожие на пение птиц. Благодаря разнообразию звуков можно было даже определить точное местонахождение злоумышленника в замке.

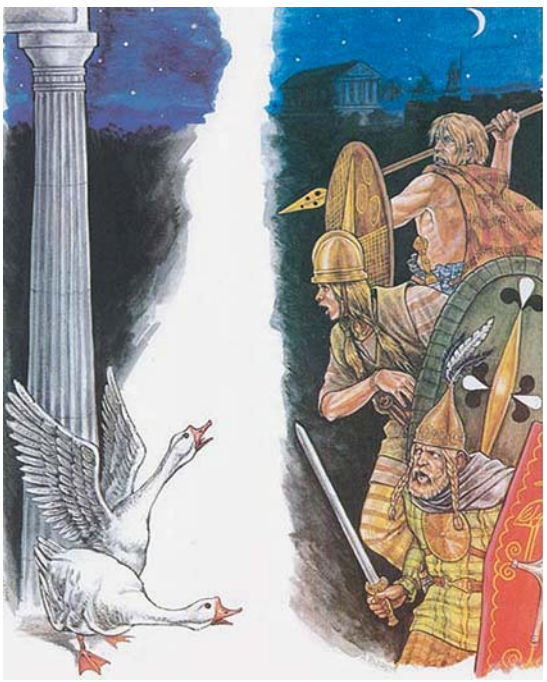
Но в данной статье речь пойдет об электрических системах охранной сигнализации, которые появились в XIX в. после изобретения электрического звонка. Именно о такой системе охраны думал герой рассказа М. Зощенко «Ночное происшествие», написанного в 1940 г. Прогуливаясь по ночному городу, он услышал

голос старого мужчины, звавшего его. Оказалось, что этот мужчина — сторож, которого заперли в магазине, чтобы он охранял его. Сторож просил воды. На вопрос героя рассказа, почему же тот сам не может сходить за ней, он ответил, что заперт между двумя дверьми — в магазин и со стороны улицы. Дверь со стороны улицы защищала его от вора, а в магазин была дверь заперта для того, чтобы вор не проник внутрь, пока сторож отошел или уснул. Героя рассказа возмутило то, что для этих целей используют живого человека, долго он ворочался и не мог уснуть от мысли, почему до сих пор не изобрели электрический прибор, чтобы тот оповестил о проникновении злоумышленника. Такойе техническое средство действительно было бы хорошим решением для этой ситуации. В то время Зощенко еще не мог знать, что охранная сигнализация уже была изобретена.

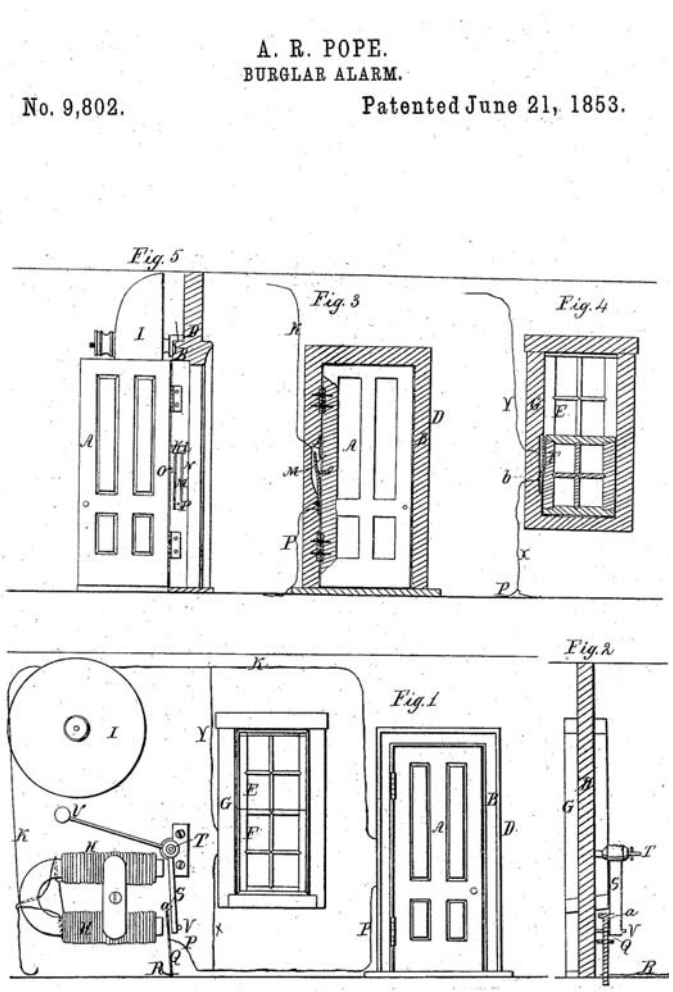
Первые периметральные сигнализации были механическими. Они работали по принципу «Патентованной сигнализации от грабителей и ловушки для животных» Джорджа Пратта. По периметру натягивалась проволока или веревка, удерживающая груз над бойком с пороховым зарядом. При обрыве проволоки груз падал, и порох взрывался, оповещая охрану о нарушении периметра.

«Отцом» электрической охранной сигнализации по праву может считаться Альберт Августус Поуп (Pope Albert Augustus) из американского Сомервилля. Летом 1853 г. он запатентовал первую электрическую сигнализацию, работавшую за счет аккумулятора, электромагнита и колокола. Она оказалась значительно надежнее, чем механическая сигнализация, в которой тяга от датчиков приводила в движение обыкновенный будильник на пружине. Запатентованная периметральная сигнализация была одношлейфовой: соединенные контакты всех окон и дверей составляли единую цепь, при открытии одного из элементов контакты замыкались, подавая ток на электромагнит, обеспечивающий звон колокола.

Но идея Поупа оставалась «на бумаге» до тех пор, пока в 1857 г. Эдвин Холмс (Edwin Holmes) не приобрел его патент за $1,5 тыс. и не наладил производство на своей фабрике в Бостоне. Поначалу люди довольно скептически относились к использованию электрической сигнализации в домах, и бизнес не приносил прибыли. Поэтому через пару лет Холмс в поисках нового, крупного рынка переместил бизнес в Нью-Йорк, где в то время процветали воровство и грабеж. К 1866 г. он установил



▲ Гуси спасают Рим от галлов. Художник А. Каращук



◀ Схема запатентованной электрической сигнализации Поупа

▶ Эдвин Холмс

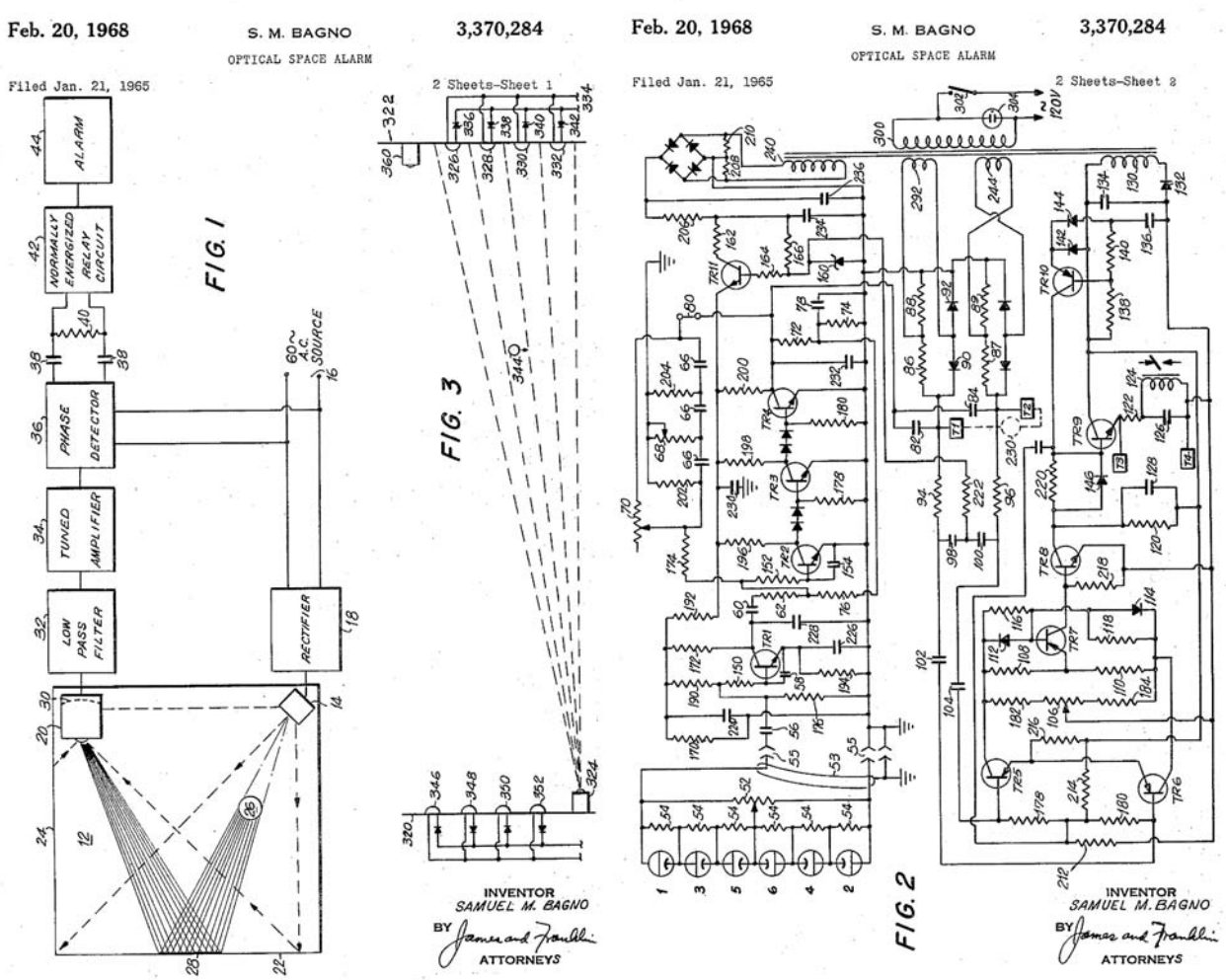
уже 1200 охранных сигнализаций в домах и квартирах и начал проводить маркетинговую кампанию для коммерческих предприятий. Через несколько лет он установил первую систему охранных сигнализаций, сигнал тревоги с которой поступал по телефонному кабелю в ближайший пункт полиции. В результате к концу XIX в. практически все особо значимые объекты были оснащены охранной сигнализацией.

После изобретения фотоэлемента в 90-х годах XIX в. популярность охранных систем резко возросла благодаря повышению ее эффективности. Теперь для прерывания цепи достаточно было перекрыть источник света, который падал на нее, а на этом злоумышленнику попасться было гораздо проще, чем на повреждении цепи проводов. В таком типе охранной сигнализации использовались светолучевые сигнализаторы. Луч света, падающий на фотоэлемент, являлся «воздушным» охранным проводом, который посылал сигнал тревоги при его нарушении.

Появлению принципиально новых систем охранной сигнализации способствовали достижения в смежных областях физики, изобретение полупроводников и резкий скачок в развитии радиоэлектроники в 50–60-х годах. Постепенно световые лучи и фотоэлементы начали замещаться ультразвуковыми датчиками, которые вычисляли время, требующееся звуку для движения от датчика до, например, стены и обратно до датчика, либо проверяли, был ли получен отправленный сигнал отдельным приемником. В 1953 г. американский изобретатель Самуэль Багно (Samuel Bagno) запатентовал первый ультразвуковой датчик движения, в котором использовались принцип действия радара, свойства ультразвуковых волн и эффект Доплера.

За ультразвуковыми датчиками последовали микроволновые (объемные) датчики, которые излучают высокочастотные микроволновые

▼ Схема запатентованного Самуэлем Багно ультразвукового датчика движения



волны, которые, отражаясь от окружающих объектов, регистрируются сенсором, а микропроцессор устройства, в случае обнаружения даже малейших изменений отраженных электромагнитных волн, приводит в действие заложенную в него функцию. То есть, когда в зоне обнаружения такого датчика появляется движущийся объект, мгновенно формируется сигнал тревоги.

В 70-е годы был создан инфракрасный датчик, принцип работы которого заключался в обнаружении изменений теплового (инфракрасного) излучения объектов. Теперь злоумышленнику, пробравшемуся на территорию, которая оборудована сигнализацией с такими датчиками, стало почти невозможно избежать обнаружения.

Благодаря современным достижениям в сфере ИТ, охранная сигнализация становится все более функциональной и простой в управлении. Так, владелец охраняемого объекта с помощью мобильного телефона имеет возможность включать/отключать систему сигнализации, регулировать освещение, включать системы отопления, вентиляции и полива.

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ (СКУД)

Человек всегда стремился ограничить доступ чужаков на его территорию — с помощью замков со сложными личинками, потайных замочных скважин, сооружений вокруг замков и крепостей, рвов, всяческих западней и даже медвежьих капканов. Это и были первые системы контроля доступа.

Первый в истории человечества ключ выглядел как небольшая палочка с колышками. Именно такой ключ был найден в гробнице египетского фараона Рамзеса II. Колья-шипы, находящиеся на палке, подходили к задвижке с дырочками. В Греции структуру ключа усовершенствовали, и она стала похожа на «монтировку»: небольшая трубочка с язычком на конце, который совмещался с пазом на засове.

Довольно долго человечество не могло продвинуться в конструировании систем контроля доступа дальше кодовых замков и турникетов, которыми (обычно при помощи педали) управляли вахтеры. Возросшая в XX в. преступность послужила мощным толчком к развитию и совершенствованию СКУД. В 80-е годы на смену металлическим ключам пришла перфорированная ключ-карта (punched-hole card). Система работала следующим образом: на пластиковой карточке-ключе имелось порядка 15 отверстий (у разных ключей — разные комбинации отверстий), внутри замка помещалась копия этого ключа, при совпадении отверстий замок срабатывал, и дверь открывалась.

В 90-е годы XX в. появились электронные замки, в которых вместо ключа стали использовать пластиковую карту с магнитной полосой. Электронные системы замков для помещений позволили забыть о потерянных ключах и нелегальном изготовлении их копий, к тому же, помимо этого, значительно расширились возможности контроля. Система автоматически формирует отчеты обо всех событиях: выдача ключей; время входа и выхода из помещений, о личностях, входивших в помещение.

Современные достижения в области автоматизированных систем контроля доступа обладают рядом преимуществ. Во-первых, это минимизация влияния человеческого фактора, который во многих случаях является причиной сбоя в охране объекта. Еще одним важным моментом является возможность интеграции всех средств обеспечения безопасности в единую систему: пожарной сигнализации, охранно-тревожной сигнализации и системы видеонаблюдения. В случае возникновения нештатных ситуаций это поможет значительно снизить время оповещения о них и существенно ускорить процесс эвакуации.

В настоящее время там, где необходим высокий уровень безопасности и хорошая функциональность (в учебных заведениях, промышленных зданиях, финансовых учреждениях и т. п.), устанавливают биометрические системы контроля и управления доступом, возможности которых до начала XXI в. применялись в большинстве случаев только спецслужбами для защиты государственной тайны, сверхважной информации и выявления особо опасных преступников.

▲ Перфорированные ключ-карты

◀ Биометрический считыватель для работы в режиме идентификации и верификации

Всегда ли биометрия оправданна?

Биометрия использует методы распознавания людей на основе их уникальных биологических и физических характеристик: ДНК человека, черты лица, сетчатка глаза, голос, походка или почерк — словом, все то, что человек не может передать кому-то или забыть дома. Самым распространенным методом является идентификация по отпечаткам пальцев.

Надежность и точность биометрических СКУД за последние несколько лет значительно выросла. Так, например, вероятность ошибочного отказа в доступе при идентификации по отпечаткам пальцев снизилась до 0,1%, а вероятность ошибочного разрешения доступа — до 0,0001%.

Выбор идентификатора зависит от целей защиты и особенностей объекта, на котором внедряется биометрическая система контроля доступа. Если планируется вводить ее на производственном предприятии, не все системы идентификации по отпечаткам пальцев подойдут, поскольку зачастую у работников по вполне понятным причинам

▼ Биометрический считыватель отпечатков пальцев со встроенным считывателем карт

► Мультифакторный биометрический терминал: распознавание отпечатков двух пальцев, распознавание лица

могут быть сильно загрязнены руки. А в местах с высокой пропускной способностью, например на проходной завода, применять биометрическую систему нецелесообразно в принципе. Но в то же время в местах массового скопления людей данную систему можно использовать для распознавания лиц преступников.

Можно ли обмануть биометрическую СКУД?

При внедрении системы контроля доступа многие задумываются о степени ее надежности. Самый частый вопрос — какова вероятность подделки идентификатора? Подделка возможна в том случае, если в алгоритме получения информации от человека и ее обработки существуют сбои или же программное обеспечение оборудования имеет изъяны. Но чаще всего подделка идентификатора не имеет смысла, т. к. злоумышленнику проще разбить окно или выломать дверь. Но там, где вопрос безопасности стоит на первом месте, установкой системы контроля доступа не ограничиваются, добавляя другие средства защиты — надежные замки, решетки на окнах и т. п.

На объектах с повышенными требованиями к безопасности необходимо использовать биометрические СКУД вместе с дополнительными идентификаторами — кодами, смарт-картами, или же использовать мультимодальные биометрические системы. Примером такой системы является идентификация по голосу и параметрам лица. При внедрении такой системы максимально снижается риск проникновения злоумышленников, поскольку становится крайне сложно подделать сразу несколько биометрических характеристик. К тому же повышается точность идентификации личности, т. к. одни биометрические признаки компенсируют недостатки, присущие другим признакам.

* * *

При обеспечении безопасности крупного предприятия или небольшого офиса нельзя делать упор лишь на одном направлении. В системе охраны важно соблюдать баланс: установив одну СКУД, нельзя забывать и о других средствах активной и пассивной защиты, а установив инженерные заграждения, следует помнить об охранной сигнализации.

В заключение необходимо напомнить, что не всегда решение, касающееся охраны, которое кажется обычному человеку наиболее логичным, является правильным с точки зрения обеспечения безопасности. Поэтому для разработки и монтажа СКУД или охранной сигнализации оправданным будет обращение к специалистам, которые учтут специфику и особенности предприятия, нуждающегося в защите от действий злоумышленника. ⬣