Примеры, демонстрирующие возможности систем запирания “**замок** + ***Lock*-охрана**”

1. Вы идете через свой приусадебный участок к входной двери дачного дома вместе с посторонним человеком (пришедшим, например, проверить показания вашего электросчетчика), достаете из-под коврика на крыльце ключ и открываете им замок входной двери.
   Но если на следующий день лжеэлектрик или его подельники попытаются без вас открыть замок этим же ключом, то у них ничего не получится, а на ваш мобильный телефон придет SMS-извещение *Тревога! Попытка взлома замка*, дублируемое дозвоном (чтобы привлечь ваше внимание именно к этой SMS-ке, т.к. мало найдется любителей *сразу же* просматривать каждое из приходящих на его телефон SMS-сообщений).
   Неудачная попытка лжеэлектрика объясняется тем, что накануне он не заметил как вы, приближаясь к дому, наступили на скрытую под травой или опавшей листвой кнопку (ну, конечно же, влагостойкую), в результате чего устройство мгновенно разблокировало ригель замка на запрограммированное вами же время (от 5 и до 250 сек.) и тем самым предоставило строго лимитированное время на открывание замка.
   Но если кто-то без нажатия на скрытную кнопку хотя бы *слегка сдвинет* ригель, то устройство без промедления отошлет на программно-заданный телефон вышеприведенное тревожное SMS-извещение, а также включит сирену, чтобы отпугнуть злоумышленника.
2. Назовите хотя бы один врезной замок (выпускаемый серийно, а не спецназначения), который сможет успешно выдержать такое испытание:
   Хорошо знакомому с устройством ***Lock*-охрана** домушнику (причем суперпрофессионалу по части *манипуляционных* методов вскрытия замков) дадим 30 минут времени для вскрытия рядового замка ***Гардиан 12.01***, в котором установлен самый простой цилиндр, но который работает в паре с устройством ***Lock*-охрана.** При этом профи может использовать любые *не разрушающие* систему запирания способы и любой имеющийся для этого инструмент, отмычки и приборы.
   После того, как он не справится с задачей, к демонстрационному стенду подойдет наш сотрудник с абсолютно *пустыми* руками, чтобы разблокировать и открыть этот замок за время порядка одной минуты. При этом на стенде вы не увидите не только дорогостоящего сканера рук или глаз, но даже обычной клавиатуры. Нет и скрытной кнопки.
   На вполне ожидаемый вопрос *А возможно ли такое?* ответим так: Скорее всего НЕТ, т.к. знающий устройство ***Lock*-охрана** домушник почти наверняка откажется возиться с замком, работающим в паре с этим устройством. А *скрытно* взломать замок или контролируемое ИК-датчиком полотно двери тоже не получится, т.к. сразу включится сирена и на записанный в память устройства телефон уйдет соответствующее тревожное SMS-извещение.
3. Один из 10-ти режимов работы инновационного устройства обеспечивает повышение секретности системы запирания “замок + ***Lock*-охрана**” до уровня, значительно превосходящего секретность банкоматов.
   В самом деле, для того чтобы банкомат выдал деньги с депозитного счета достаточно правильно воспользоваться только действующей банковской картой и 4-х значным pin-кодом.
   В то же время для разблокирования ригеля замка в этом случае необходимо будет позвонить с любого из занесенных в память устройства мобильных телефонов (звонки с незарегистрированных телефонов будут отбиты) и после “поднятия трубки” устройством ввести DTMF-командой pin-код.
   И только если все это было сделано правильно, устройство на программно-заданное время активирует считыватель RFID-карт. Разблокирование ригеля произойдет при прикладывании к нему одной из зарегистрированных RFID-карт, секретность которых выше секретности банковских карт с магнитной полосой. После чего замок можно будет открыть его штатным ключом.

Т.е. для открывания замка в этом режиме надо успешно преодолеть 4 рубежа/степени защиты:

***звонок с моб. тлф. → ввод pin-кода→ RFID-карта→ штатный ключ*.**

В то время как для снятия денег в банкомате достаточно преодолеть только 2 рубежа защиты:

вставить в считыватель банковскую карту и ввести pin-код.

Но если всего два рубежа защиты неплохо оберегают многочисленные банкоматы от несанкционированного снятия денег, то что можно сказать о секретности системы запирания с четырьмя рубежами защиты! Особенно, если принять во внимание то обстоятельство, что после двух-шести неправильных попыток ввода pin-кода (их количество назначается программно) или незарегистрированных RFID-карт устройство поднимет тревогу и, что ещё важнее, будет игнорировать в течение программно-заданного времени (от 5-ти и до 256 мин.) дальнейшие попытки разблокирования.

4. И, наконец, если даже та степень секретности запирающей системы, которая описана в предыдущем примере, кому-то покажется недостаточной, то можно поставить на двери ещё и дополнительный электромеханический замок (например, CISA 1A731), который будет открываться электрическим сигналом, приходящим с релейного выхода ***Lock*-охраны** после получения устройством ещё одной DTMF-команды (т.е. речь идет уже о 5-м рубеже охраны!).