**Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):63-64**
**Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667**

# SMART-LOCK AND DANGER FOR ITS OWNER

**B.Horbatenko, V.Stopin**
*Kharkiv National University of Radio Electronics (NURE), Kharkiv, Ukraine*

**ABSTRACT.** Demand for digital technology still has strong positions on the market. Every single year more and more modern technologies introduced in our lives. Command Spot company conducted a survey with the main question: “Which smart device do you want to use in your surrounding?”. The most common answer was smart-lock. But, do responders think thoughtful about this gadget security? Dangers that hide behind the smart locks and marketing slogans of companies are proposed in this paper.

**Аннотация.** Спрос на цифровые технологии не перестает утихать. С каждым годом появляются все более новые технологии, которые внедряются (в прямом смысле этого слова) в нашу жизнь. Компанией Command Spot был проведен опрос, в ходе которого был задан вопрос – какое умное устройство Вы бы хотели подключить себе в первую очередь? – респонденты на первое место (48%) поставили умный замок. Однако задумывались ли респонденты о безопасности данного гаджета? Данная статья описывает опасности, которые скрываются за умными замками и маркетинговыми лозунгами компаний.

***KEYWORDS:*** Smart house, IOT, Internet of things, Smart lock, Security, Gadget.

Все мы стремимся иметь в своем арсенале наиболее новую цифровую «игрушку», в которую внедрены какие-либо функции или внешние составляющие, которых нет в других гаджетах. Кто-то придумывают новые фонарики или маячки, кто-то незначительно улучшает качество изображения на гаджете, а другие – прикручивают к велосипеду третий руль. Последние примеры не всегда являются самыми хорошими особенностями. А некоторые разработки совсем не должны появляться в общем доступе.
В данной статье не будут рассмотрены конкретные цифровые замки, по той причине, что в большинстве случаев их принцип работы, протоколы безопасности и составляющие являются частично, а иногда и полностью идентичными.

«Смарт-замок» – это довольно сложный термин, охватывающий широкий спектр технологических новшеств. Технические и программные особенности продукции на рынке являются часто закрытыми для покупателей, но зато есть маркетинговые надписи, где создатели того или иного смарт-замка гарантируют полную безопасность своего продукта.

Для смарт-замков требуются сменные батареи, что зачастую может стать проблемой. Почему? Представьте, что вы уехали на долгий отдых в другую страну и в один из дней батарея на вашем «умном» замке перестанет работать. Это приведет к отключению системы и вытекающими с ней последствиями.

Смарт-замки в своем большинстве никаким образом не защищены от возгораний. Таким образом, в случае возникновения пожара, ваш замок может просто сгореть. Дальнейшее его функционирование, как и ваша безопасность, остаются под угрозой.
Ремонт подобных смарт-замков является очень затруднительным, так как первый попавшиеся мастер не сможет отремонтировать ваш замок. Только специализированные сервисы, которые относятся к компании-поставщику, имеют возможность отремонтировать замки собственного производства, то есть потребитель сильно привязан к компании поставщику, а если замок приобретен из-за границы?

Удаленное управление посредством сети – это один из самых худших вариантов вашей безопасности. Производители не предоставляют открытый доступ к исходному коду устройств, которые они продают потребителям. Таким образом, производитель может внедрить backdoor в систему и эксплуатировать её удаленно. Полиции необходимо открыть дверь? – дверь открыта. Множество производителей пытаются отходить от подобных методов управления и находить более безопасные пути реализации удаленного управления, например, посредством использования низкой энергии bluetooth, что дает некоторые дополнительные функции безопасности, которых нет в исходном протоколе. Однако, несмотря на то, что в целом данный протокол себя относительно неплохо зарекомендовал, выполнение команд и связанные с ним сопутствующие приложения, выпущенные производителями замков, не так уж хороши. В тестах, проведенных Defcon в 2016 году, 12 из 16 моделей смарт-замков провалили тест при устойчивой атаке. Большинство из этих провалов касались либо реализации шифрования, либо низкопробного кода в сопутствующих приложениях.

Исходя из плохой конструкции и реализации защиты «смарт» устройства, подобные этим, как правило, имеют нечеткие правовые границы, связанные с владением и обслуживанием. Относительно недавно, во время приобретения, была закрыта компания по автоматизации домов, под названием Revolv. И вместо того, чтобы просто не предоставлять обновления своим потребителям, устройства были отключены. Это привело пользователей к значительным неудобствам. Таким образом, каждая компания, предоставляющая подобные устройства, в один момент может прекратить свое существование и поставить под угрозу безопасность вас и вашего имущества.
Итак, подводя итог, у стандартных замков, которые до сих пор используются большинством из нас, однозначно есть недостатки в безопасности, но все они имеют единый комплекс дизайна, общепринятые стандарты, по которым они оцениваются, и могут быть отремонтированы или заменены кем-либо и принадлежат только вам, без какого-либо удаленного управления. Могут ли смарт-замки сказать то же самое? Решать вам.

## REFERENCES

- https://geektimes.ru/post/266720/