Исследование уязвимостей систем умного дома и поиск путей обеспечения их безопасности

Автор разработки студент 2 курса

БУ «Няганского технологического колледжа»

Фурцев И.Б


ОГЛАВЛЕНИЕ

Актуальность

- Большинство систем автоматизации умных зданий не имеют полноценной системы защиты от кибернетических атак. Большинство решений по защите связано с установкой стандартных программ, выполняющих только функции сетевого экрана. Но в случае с атаками на системы автоматизации зданий этого недостаточно. Вышеперечисленные факторы и обусловили выбор темы исследования в качестве актуальной.

Цель

- Цель данного проекта – исследовать пути обеспечения безопасности систем Smarthouse.
- Объектом исследования данной работы является система Smarthouse.
- Предметом исследования выступает система высокотехнологичных устройств в здании современного типа.

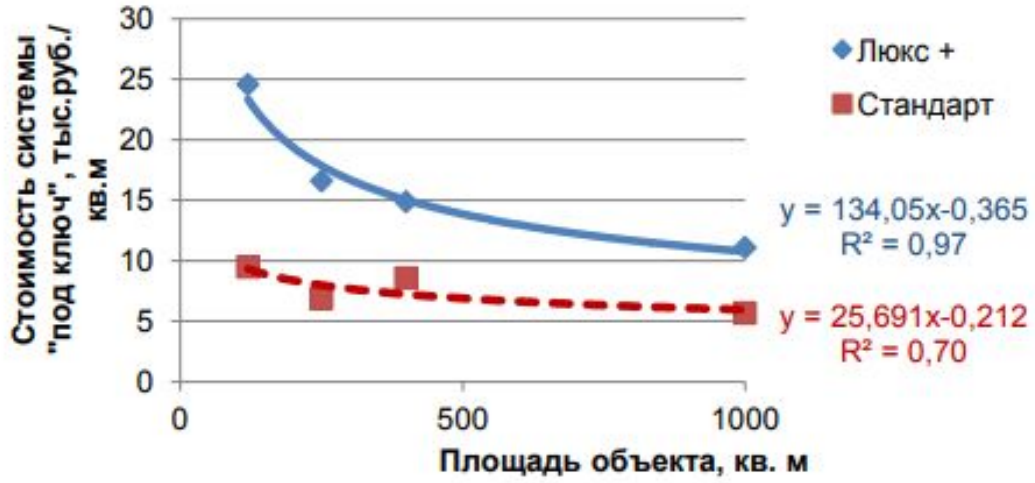
Гипотеза

- Классифицировав угрозы интернет безопасности, выявив их особенности и пути достижения неуязвимостей, доля доверия людей к применению систем умный дом повысится, что приведет к успешной реализации направления политики государства «Умный город».

Перспективы «умных» домов в России

Использование систем «умного дома» в России

- Использование систем «умного дома» домохозяйствами находится в России крайне низок – менее 0.1% от общего количества квартир и индивидуальных жилых домов.
- Обзор предложений типовых проектов системы «умный дом» в городе-миллионнике Санкт-Петербурге позволил получить степенную зависимость удельной стоимости установки от площади объекта.



Интерес к «Умному дому»

- Уже сейчас в России наблюдается увеличенный интерес к установке систем умного дома. Согласно данным опроса Hi-Tech Mail.ru на начало 2020 года 88% россиян знают, что такое умный дом, но используют новые технологии лишь 27%.

Среди брендов умных домов лидирует Xiaomi

Ранг	Бренд	Запросы
1	Xiaomi	96 634
2	Ростелеком	36 418
3	Мегафон	11 775
4	Redmond	8 759
5	Rubetek	6 507
6	Apple	4 957
7	MTC	4 138
8	Samsung	2 534

Данные Яндекса. Июль 2018

Система управления умным домом

Перечень систем управления по основным признакам:

- Проводные
- Беспроводные
- Централизованные
- Децентрализованные
- С открытым протоколом
- С закрытым протоколом

Уязвимость систем умного дома

Слабое шифрование данных внутри системы «Умный дом»

Потенциальные уязвимости системы «Умный дом» ввиду функционирования в ней устройств от разных производителей

Отсутствие механизма аутентификации санкционированного пользователя

Необходимость наличия защищенных каналов связи

Наличие свойственных определенным устройствам уязвимостей информационной безопасности

Пути обеспечения безопасности умного дома

- Задачи:
  - прогнозирование, обнаружение и оценка информационных угроз;
  - совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности.

Факторы классификации угроз интернет-безопасности

- уровень опасности последствий реализации угрозы;
- цели и мотивация источников угроз;
- носитель угрозы;
- признаки проявления реализации угрозы;
- механизмы и инструменты реализации угрозы.

Классификатор угроз ИБ

Схема удаленного управления системой Smarthouse

Пути обеспечения безопасности умного дома

Обеспечения безопасности роутера

Повышение уровня безопасности и организация соответствующей степени защиты своего маршрутизатора должны быть для пользователей приоритетным первым шагом.

Если производитель роутера не предлагает новую прошивку, то стоит убедительно задуматься о замене маршрутизатора на более новую и современную модель.

Использование уникальных паролей для каждого устройства

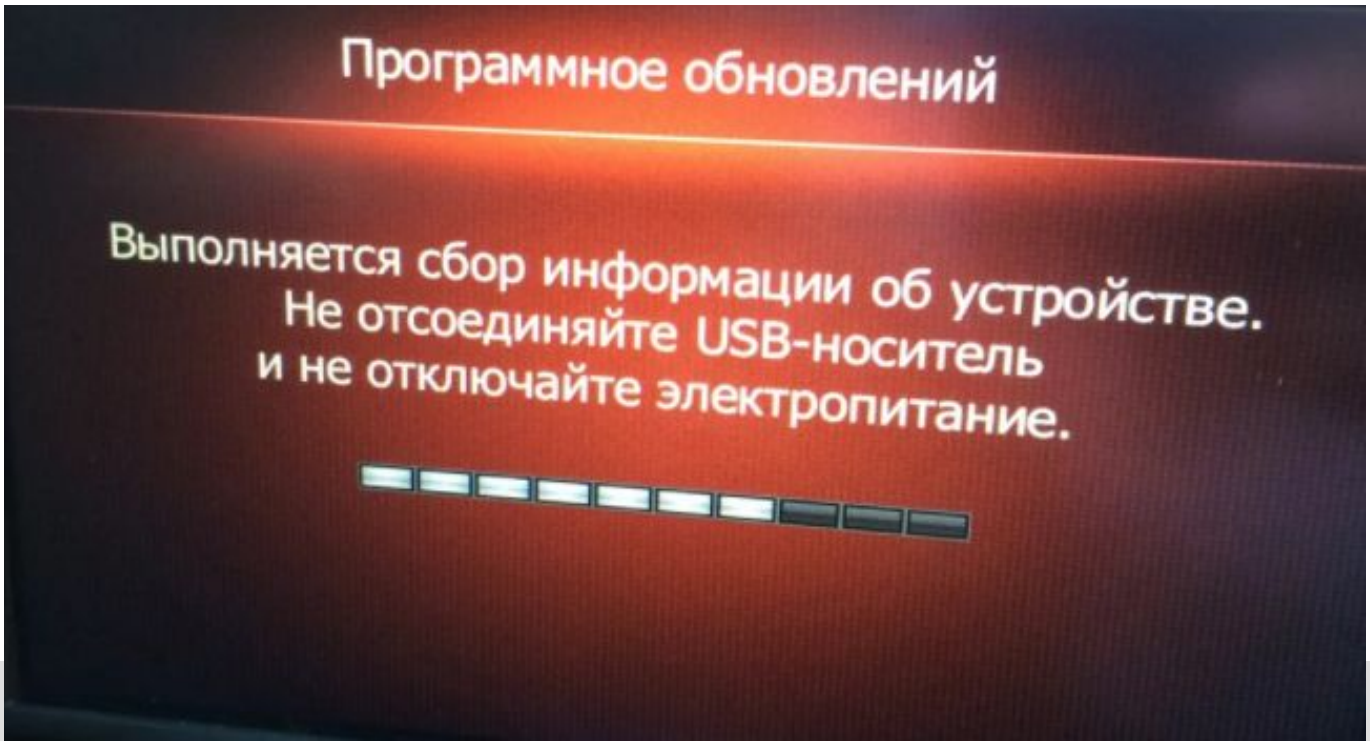
Каждое устройство должно иметь уникальный сложный комбинированный пароль. Если определенная действующая парольная фраза будет использоваться повторно в службах и устройствах «умного дома», пользователи рискуют получить общий единый скомпрометированный блок, что приведет к появлению дополнительных точек уязвимости в пользовательской системе управления.

Включение двухфакторной аутентификации для всех возможных устройств

Двухфакторная аутентификация – это дополнительный уровень безопасности помимо применения простого пароля. При использовании режима двухфакторной аутентификации, после того, как пользователи введут свой пароль, им придется дополнительно удостоверить свою личность, согласованным ранее, способом.

Регулярное обновление прошивки на всех своих устройствах

Обязательное обновление прошивки программной платформы необходимо выполнять на регулярной основе не только непосредственно для маршрутизатора, но и всех задействованных устройств «умного дома».



Приобретение устройств только от известных и доверенных компаний

Применение продукции от крупной известной компании также не гарантирует, что в дальнейшем подобного с ней не произойдет. Однако пользователи могут6

- ✔ ознакомиться с послужным списком компаний
- ✔ просмотреть историю выпуска продуктов
- ✔ проанализировать ее жизнеспособность
- ✔ изучить граничные временные рамки гарантированной поддержки компанией своих продуктов.

Не управлять своим «умным домом» из общедоступной сети «Wi-Fi»

Не рекомендуется использовать публичную сеть «Wi-Fi» для удаленного доступа к своему «умному дому», даже если присутствует уверенность, что сеть «Wi-Fi» гарантированно безопасна.

ЗАКЛЮЧЕНИЕ

Программные антивирусные продукты не могут решить задачу полной защиты системы автоматизированного здания ввиду отсутствия аппаратной составляющей комплекса. Можно утверждать, что существующие программные антивирусы не позволяют полностью защитить систему. Таким образом, создание антивирусной системы, способной обеспечивать комплексную защиту системы автоматизированного управления зданием — это задача ближайших лет

Спасибо!