Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
Vol. 4, Is. 2, pp. 48-54, 2015

DOI: 10.13187/vesp.2015.4.48
www.ejournal21.com

Technical Means

UDC 004.056

«Smart Home» Risk Analysis

[1] Alexander A. Efremov
[2] Catherine E. Bessonova

[1] National research university of information technologies, mechanics and optics, Russian Federation
197101, Saint Petersburg, Kronverkskiy prospekt, 49
E-mail: alexandrovefim@mail.ru
[2] National research university of information technologies, mechanics and optics, Russian Federation
197101, Saint Petersburg, Kronverkskiy prospekt, 49
PhD in Engineering sciences, Assistant
E-mail: merom812@gmail.com

Abstract

This article reveals the problem of insecurity of systems based on the technology of «Smart home». There is given the analysis and risk assessment, developed recommendations for improving the security of smart homes. Compliance with these guidelines will significantly increase the level of security systems based on the technology of "smart house" that will solve the problem partially vulnerability of this type of system, which at the moment is quite acute.

Keywords: information security, smart home, risk management, threats and vulnerabilities.

Введение

Технологии умного дома в настоящий момент очень активно набирают популярность. Составной частью «Умного дома» являются различного рода сигнализации и датчики (например, датчики движения, задымления, датчики открытых дверей и окон, системы видеонаблюдения), которые помогают обеспечить безопасность квартир, коттеджей и других жилых помещений, в которых установлены данные системы. Также существует возможность внедрения специального встраиваемого оборудования, используемого правоохранительными органами и частными охранными предприятиями, которое позволяет отслеживать неразрешенную деятельность на контролируемой территории [1, 2, 3].

Но, к сожалению, помимо большого числа преимуществ данной системы она имеет и ряд недостатков. Согласно ряду исследований, данному типу систем присущ ряд уязвимостей [4, 7, 8, 9]. Также, в настоящее время прогнозируется рост числа правонарушений, связанных с умной техникой в целом и умными домами в частности. [10]

Задачей исследования является выявление наиболее уязвимых частей «Умного дома», идентификация и оценка рисков, актуальных для данного типа систем, а также выработать рекомендации по воздействию на них.

Результаты

В основе исследования был положен государственный стандарт *ISO 27005 – Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности*. [11] Для возможности его применения в проведенном исследовании пришлось адаптировать процесс управления рисками. В итоге использовалась следующая схема.

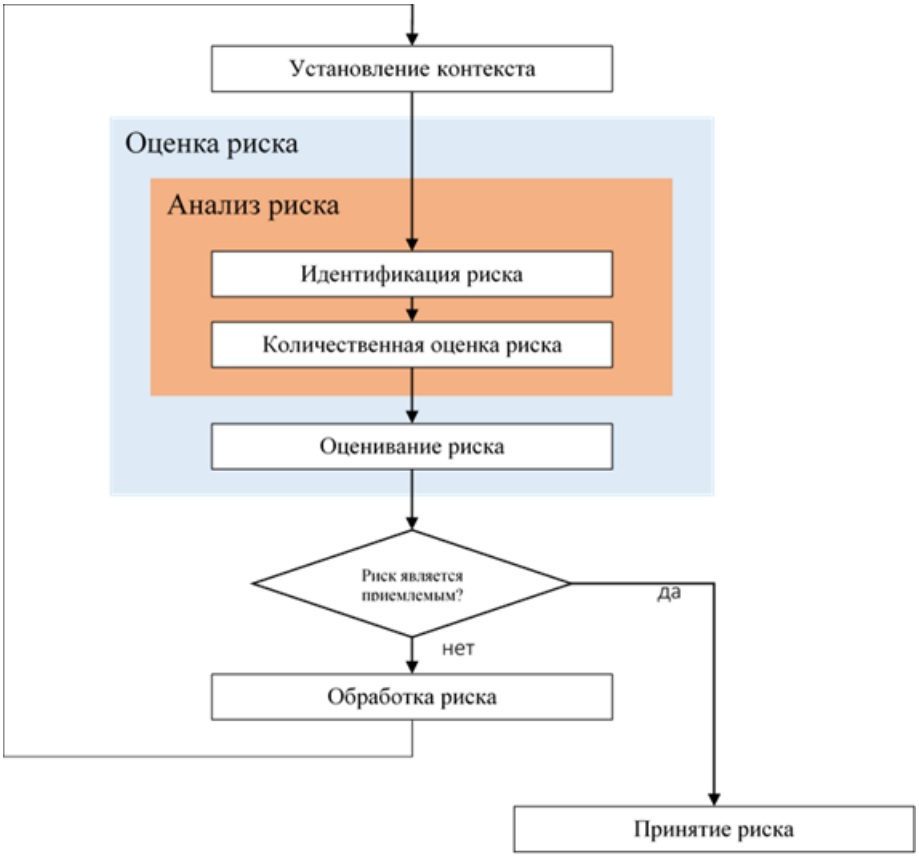

Рис. Используемая в работе схема управления рисками

На этапе установления контекста были определены шкалы для проведения экспертных оценок, а также ценность нарушаемых свойств актива.

На этапе идентификации риска в результате экспертной оценки были идентифицированы уязвимости, актуальные для систем, построенных по технологии Умный дом. Для проведения данной оценки были привлечены 5 экспертов. Актуальной признавалась уязвимость, если за нее проголосовало 3 и более экспертов. В результате актуальными были признаны 25 уязвимостей. Ниже приведен фрагмент таблицы, содержащей мнения экспертов по определению актуальных уязвимостей.

Таблица 1. Экспертные оценки по идентификации уязвимостей

Уязвимость	Мнения экспертов (№):				
	1	2	3	4	5
Незащищённые линии связи	+	+	+	+	+
Нехватка установленных контрольных механизмов в случае нарушений правил безопасности	+				+
Передача паролей в открытом виде	+	+	+		+
…					

После идентификации актуальных уязвимостей было определено, какие свойства актива (конфиденциальность, целостность, доступность) могут нарушать те или иные угрозы (Таблица 2), далее было произведено сопоставление угроз и уязвимостей (Таблица 3).

Таблица 2. Соответствие угроз и нарушаемых ими свойств актива

Угроза	Свойства, которые угроза может нарушить		
	К	Ц	Д
Программный сбой			+
Перехват и подмена передаваемого сигнала	+	+	
Вмешательство в аппаратные средства	+	+	+
…			

Таблица 3. Сопоставление угроз и эксплуатируемых ими уязвимостей

Угроза	Уязвимость
Хищение документов и носителей информации	Недостатки физической защиты здания, окон и дверей
	Неадекватное и небрежное использование физического контроля доступа к зданию и помещениям
	Незащищенное хранение
Ошибка в использовании	Отсутствие или недостаточность механизмов мониторинга
	Недостаточность изучения вопросов безопасности
…	

Следующим этапом являлось определение актуальных угроз. Актуальными считались угрозы, которые нарушали хотя бы одно из свойств актива (конфиденциальность, целостность или доступность), а также могут быть реализованы путем использования, как минимум, одной актуальной уязвимости. Всего было идентифицировано 27 актуальных угроз. Наиболее опасными из них можно считать следующие: фальсификация прав, искажение данных, вмешательство в программные средства, перехват и подмена передаваемого сигнала, т.к. для реализации данных угроз можно воспользоваться наибольшим числом различных актуальных уязвимостей.

В результате сопоставления актуальных угроз, уязвимостей, используемых при реализации данных угроз и нарушаемых свойств актива было идентифицировано 233 риска.

Таблица 4. Идентифицированные риски

ID	Свойство актива	Угроза	Уязвимость
1	Д	Причинение ущерба огнем/пожаром	Недостатки физической защиты здания, окон и дверей
2	Д	Значительный инцидент (авария)	Чувствительность к перепадам напряжения
3	Д	Значительный инцидент (авария)	Недостатки физической защиты здания, окон и дверей
4	Д	Уничтожение оборудования или носителей	Незащищенное хранение
5	Д	Уничтожение оборудования или носителей	Неправильное использование программного обеспечения и оборудования
...			

Далее, путем экспертной оценки были определены уровни идентифицированных рисков. В результате были получены риски с уровнями от 4 до 9. Неприемлемыми были признаны риски с уровнями 7 и выше. Таким образом, было идентифицировано 189 неприемлемых рисков.

Для обработки этих рисков было выработано 22 рекомендации, которые позволят повлиять на все 189 неприемлемых рисков. Ниже приведены рекомендации, которые позволят повлиять на наибольшее число рисков:

1) Использование в системе "Умный дом" системы разграничения доступа к объекту.
2) Хранение и передача паролей только в зашифрованном виде. Ограничение доступа к таблицам паролей.
3) Использование шифрования передаваемых сигналов.
4) Предварительная проверка закупочных материалов, окон и дверей.
5) Периодический пересмотр прав доступа к управлению системой "Умный дом"
6) Использование в системе "Умный дом" систем обнаружения вторжений и межсетевых экранов.
7) Постоянный мониторинг наличия недостатков и уязвимостей ПО, и своевременное устранение обнаруженных уязвимостей и недостатков.
8) Обеспечение невозможности свободного доступа к аппаратной части системы "Умный дом".
9) Использование разграничения доступа к управлению системой "Умный дом".
10) Периодический пересмотр прав доступа к объекту.

Заключение

Таким образом, была исследована проблема незащищенности систем «Умного дома», их текущее состояние в мире информационных технологий, а также приоритет данного направления для вневедомственных подразделений и частных охранных предприятий. В ходе проделанной работы был видоизменен процесс управления рисками до необходимого уровня.

В результате были идентифицированы угрозы, характерные для систем, построенных по технологии «Умный дом», а также актуальные уязвимости. На основе идентифицированных угроз, уязвимости и ценности рассматриваемого актива были идентифицированы актуальные риски. Всего было идентифицировано 233 риска. Часть из них была признана приемлемыми и не подлежащими обработке. Для остальных были предложены меры по их обработке. Всего было предложено 22 меры, которые помогут снизить уровни перечисленных рисков до приемлемых.

Результатом проделанной работы можно считать выработку рекомендаций, необходимых для снижения существующих рисков. Соблюдение данных рекомендаций

позволит существенно повысить уровень защищенности систем, построенных по технологии «Умный дом», что частично позволит решить проблему незащищенности данного типа систем, которая на данный момент является довольно острой.

Примечания:

1. Обзор систем и технологий "Умный дом" [Электронный ресурс] – URL: http://www.a3d.ru/design/tehnolog/25 режим доступа: свободный (дата обращения 08.05.2015).

2. "Umnyi dom" - marketingovyi issledovanie rossiiskogo rynka: tekushchee sostoyanie i prognoz razvitiya. [Elektronnyi resurs] – URL: http://www.directinfo.net/index.php?option =com_content&view=article&id=139%3A2010-07-06-13-57-09

3. Smart Homes Market. [Elektronnyi resurs] –URL: http://www.prweb.com/ releases/smart-homes-market-2020/analysis-and-forecasts/prweb11302579.htm

4. Бессонова Е.Е., Ефремов А.А., Настека А.В., Овсяникова В.В., Салахутдинова К.И., Трофимов А.А. Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ «УМНЫЙ ДОМ» // Региональная информатика «РИ-2014» Материалы конференции 2014. (124). [Электронный ресурс] – URL: spoisu.ru/ri/ri2014/ri2014_materials.pdf режим доступа: свободный (дата обращения 08.05.2015)

5. Ефремов А.А, Настека А.В., Овсяникова В.В., Салахутдинова К. И., Трофимов А.А. Защита системы «Умный дом» от программных сбоев // Сборник тезисов докладов конгресса молодых ученых. [Электронное издание] – URL: http://kmu.ifmo.ru /collections_article/1011/ zaschita_sistemy_%C2%ABumnyy_ dom%C2%BB_ot_ programmnyh _sboev.htm

6. Ефремов А.А, Настека А.В., Овсяникова В.В., Салахутдинова К. И., Трофимов А.А. Защита управляющих сигналов в системе «Умный дом» // Сборник тезисов докладов конгресса молодых ученых. [Электронное издание] – URL: http://kmu.ifmo.ru/ collections_article/1013/ zaschita_upravlyayuschih_signalov_v_sisteme_«umnyy_dom».htm

7. Снегуров А.В., Ткаченко Е.А., Кравченко А.Д. Риски информационной безопасности систем, построенных по технологии «Умный дом» // ВЕЖПТ . 2011. №3 (52). [Электронный ресурс] URL: http://cyberleninka.ru/article/n/riski-informatsionnoy-bezopasnosti-sistem-postroennyh-po-tehnologii-umnyy-dom режим доступа: свободный (дата обращения: 08.05.2015).

8. Mario Ballano Barcena, Candid Wueest Insecurity in the Internet of Things [Электроныйй ресурс] – URL: http://www.symantec.com/content/en /us/enterprise /media/ security_response/whitepapers/insecurity-in-the-internet-of-things.pdf режим доступа: свободный (дата обращения 08.05.2015)

9. Michael S., Ulf L., 7 Smart-Home-Starter-Kits im Sicherheits-Test // AV-TEST-Studie. – 2014. P. 16-41.

10. Аналитический отчет о ключевых тенденциях в сфере информационной безопасности [Электронный ресурс] – URL: http://www.esetnod32.ru/company /press/center/eset-2014-god-prineset-bum-tekhnologiy-anonimnosti/ режим доступа: свободный (дата обращения 08.05.2015)

11. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

References:

1. Obzor sistem i tekhnologii "Umnyi dom" [Elektronnyi resurs] – URL: http://www.a3d.ru/design/tehnolog/25 rezhim dostupa: svobodnyi (data obrashcheniya 08.05.2015).

2. "Umnyi dom" - marketingovyi issledovanie rossiiskogo rynka: tekushchee sostoyanie i prognoz razvitiya. [Elektronnyi resurs] – URL: http://www.directinfo.net/index.php?option= com_content&view=article&id=139%3A2010-07-06-13-57-09

3. Smart Homes Market. [Elektronnyi resurs] –URL: http://www.prweb.com/releases /smart-homes-market-2020/analysis-and-forecasts/prweb11302579.htm

4. Bessonova E.E., Efremov A.A., Nasteka A.V., Ovsyanikova V.V., Salakhutdinova K.I., Trofimov A.A. Rossiya, Sankt-Peterburg, Sankt-Peterburgskii natsional'nyi issledovatel'skii universitet informatsionnykh tekhnologii, mekhaniki i optiki ANALIZ ZAShchISHchENNOSTI SISTEM «UMNYI DOM» // Regional'naya informatika «RI-2014» Materialy konferentsii 2014. (124). [Elektronnyi resurs] – URL: spoisu.ru/ri/ri2014/ri2014_materials.pdf rezhim dostupa: svobodnyi (data obrashcheniya 08.05.2015)

5. Efremov A.A, Nasteka A.V., Ovsyanikova V.V., Salakhutdinova K. I., Trofimov A. A. Zashchita sistemy «Umnyi dom» ot programmnykh sboev // Sbornik tezisov dokladov kongressa molodykh uchenykh. [Elektronnoe izdanie] – URL: http://kmu.ifmo.ru/collections_article/1011/zaschita_sistemy_%C2%ABumnyy_dom%C2%BB_ot_programmnyh_sboev.htm

6. Efremov A.A, Nasteka A.V., Ovsyanikova V.V., Salakhutdinova K. I., Trofimov A. A. Zashchita upravlyayushchikh signalov v sisteme «Umnyi dom» // Sbornik tezisov dokladov kongressa molodykh uchenykh. [Elektronnoe izdanie] – URL: http://kmu.ifmo.ru/collections_article/1013/ zaschita_upravlyayuschih_signalov_v_sisteme_«umnyy_dom».htm

7. Snegurov A.V., Tkachenko E.A., Kravchenko A.D. Riski informatsionnoi bezopasnosti sistem, postroennykh po tekhnologii «Umnyi dom» // VEZhPT . 2011. №3 (52). [Elektronnyi resurs] URL: http://cyberleninka.ru/article/n/riski-informatsionnoy-bezopasnosti-sistem-postroennyh-po-tehnologii-umnyy-dom rezhim dostupa: svobodnyi (data obrashcheniya: 08.05.2015).

8. Mario Ballano Barcena, Candid Wueest Insecurity in the Internet of Things [Elektronyni resurs] – URL: http://www.symantec.com/content/en/us/enterprise/media/ security _response/whitepapers/insecurity-in-the-internet-of-things.pdf rezhim dostupa: svobodnyi (data obrashcheniya 08.05.2015)

9. Michael S., Ulf L., 7 Smart-Home-Starter-Kits im Sicherheits-Test // AV-TEST-Studie. – 2014. P. 16-41.

10. Analiticheskii otchet o klyuchevykh tendentsiyakh v sfere informatsionnoi bezopasnosti [Elektronnyi resurs] – URL: http://www.esetnod32.ru/company/press/center/eset-2014-god-prineset-bum-tekhnologiy-anonimnosti/ rezhim dostupa: svobodnyi (data obrashcheniya 08.05.2015)

11. GOST R ISO/MEK 27005-2010 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoi bezopasnosti

УДК 004.056

Анализ рисков информационной безопасности систем «Умный дом»

[1] Александр Андреевич Ефремов
[2] Екатерина Евгеньевна Бессонова

[1] Национальный исследовательский университет информационных технологий, механики и оптики, Российская Федерация
197101, Санкт-Петербург, Кронверкский проспект, 49
E-mail: alexandrovefim@mail.ru
[2] Национальный исследовательский университет информационных технологий, механики и оптики, Российская Федерация
197101, Санкт-Петербург, Кронверкский проспект, 49
Кандидат технических наук, ассистент
E-mail: merom812@gmail.com

Аннотация. Данная статья раскрывает проблему незащищенности систем, построенных по технологии «Умный дом». Проведен анализ и оценка рисков, выработаны рекомендации по повышению уровня защищенности «Умных домов». Соблюдение данных рекомендаций позволит существенно повысить уровень защищенности систем, построенных по технологии «Умный дом», что частично позволит решить проблему незащищенности данного типа систем, которая на данный момент является довольно острой.

Ключевые слова: информационная безопасность, умный дом, управления рисками, угрозы и уязвимости.