Оригинальная статья / Original article
УДК: 004.942
DOI: 10.21285/1814-3520-2016-9-58-64

ПРОЕКТИРОВАНИЕ СОВРЕМЕННОГО ЖИЛОГО ПРОСТРАНСТВА: МАТЕМАТИЧЕСКАЯ МОДЕЛЬ РИСК-ОРИЕНТИРОВАННОЙ ОЦЕНКИ БЕЗОПАСНОСТИ НА УРОВНЕ ФИЗИЧЕСКОГО ДОСТУПА

© Н.А. Овчинников[1], Е.А. Максимова[2], А.В. Алексеенко[3]
[1,2]Волгоградский государственный университет,
400062, Россия, г. Волгоград, пр. Университетский, 100.
[3]Волгоградский государственный архитектурно-строительный университет,
400074, Россия, г. Волгоград, ул. Академическая, 1.

РЕЗЮМЕ. ВВЕДЕНИЕ. Исследуются вопросы проектирования безопасного жилого пространства на уровне физического доступа. Предлагается формализованное представление модели риск-ориентированной оценки безопасности системы «Умный дом» на уровне физического доступа. Представляются результаты экспериментальных исследований влияния риск-ориентированной на интегральную оценку безопасности в исследуемой системе. **ЦЕЛЬ.** Разработать модель риск-ориентированной оценки, которая при проектировании современного жилого пространства позволит достичь требуемого уровня безопасности. **МЕТОДЫ.** Для достижения цели работы исследуются вопросы проектирования безопасного жилого пространства на уровне физического доступа на базе аппарата теории массового обслуживания. Исследуемые марковские процессы формализуются в графовой форме. Выделенные состояния системы определяют идентификационные элементы пользователя в системе «Умный дом». В структуре общей модели – модель риск-ориентированной оценки безопасности системы «Умный дом» на уровне физического доступа. **РЕЗУЛЬТАТЫ** апробации предложенной модели показали существенное влияние изменения таких показателей, как стоимость возможного ущерба от реализации соответствующей угрозы на уровне физического доступа, вероятность перехода системы из состояния S_i в состояние S_j на показатель общей безопасности системы в целом. **ВЫВОДЫ.** Предложенная модель риск-ориентированной оценки безопасности системы «Умный дом» на уровне физического доступа может использоваться как в локальном, так и в сетевом оценочном режиме, что позволяет достичь нового уровня эффективности проектного решения системы «Умный дом» в целом.

Ключевые слова: жилое пространство, «Умный дом», дерево угроз, физический доступ, риск-ориентированная оценка, интегральная оценка, формализованная модель.

Формат цитирования: Овчинников Н.А., Максимова Е.А., Алексеенко А.В. Проектирование современного жилого пространства: математическая модель риск-ориентированной оценки безопасности на уровне физического доступа // Вестник Иркутского государственного технического университета. 2016. Т. 20. № 9. С. 58–64. DOI: 10.21285/1814-3520-2016-9-58-64

DESIGNING MODERN LIVING SPACE: THE MATHEMATICAL MODEL OF RISK-ORIENTED SAFETY EVALUATION AT THE LEVEL OF PHYSICAL ACCESS

N.A. Ovchinnikov, E.A.Maksimova, A.V. Alekseenko
Volgograd State University,
100 Universitetskiy pr., Volgograd, 400062, Russia.
Volgograd State University of Architecture and Civil Engineering,
1 Akademicheskaya St., Volgograd, 400074, Russia.

ABSTRACT. INTRODUCTION. The article deals with the issues of designing a safe living space at the level of physical access. A formalized model of the risk-oriented evaluation of “Smart Home” system safety at the level of physical access is proposed. The results of experimental studies of the effect of risk-oriented safety evaluation on the integrated one in the studied system are provided. **THE PURPOSE** of this work is to develop a model of risk-oriented evaluation that will

[1]Овчинников Николай Андреевич, студент, e-mail: o.n95@mail.ru
Ovchinnikov Nikolai, Student, e-mail: o.n95@mail.ru
[2]Максимова Елена Александровна, кандидат технических наук, доцент, заведующая кафедрой информационной безопасности, e-mail: maksimova@volsu.ru
Maksimova Elena, Candidate of technical sciences, Associate Professor, Head of the Department of Information Security, e-mail: maksimova@volsu.ru
[3]Алексеенко Анна Владимировна, аспирант, e-mail: mvpuno@yandex.ru
Alekseenko Anna, Postgraduate, e-mail: mvpuno@yandex.ru

allow to achieve the required safety level while designing modern living space. **METHODS.** To achieve the set purpose the authors study the issues of designing the safe living space at the level of physical access on the basis of the queuing theory tools. Investigated Markov processes are formalized in a graph form. Distinguished states of the system determine user's identification elements in the "Smart Home" system, i.e. the model of risk-oriented evaluation of "Smart Home" system safety at the level of physical access in the structure of the general model. **THE RESULTS** of testing the proposed model have shown a significant effect of changes in the cost of possible damage from the implementation of the corresponding threat at the level of physical access and the probability of system transition from state S_i to state S_j on the total security indicator of the system as a whole. **CONCLUSIONS.** The proposed model of risk-oriented evaluation of the "Smart Home" system safety at the level of physical access can be used in both local and network evaluation mode, which allows to achieve a new effectiveness level of the design solution of the whole "Smart Home" system.
Keywords: living space, "Smart home", tree of threats, physical access, risk-oriented evaluation, integrative evaluation, formalized model

For citation: Ovchinnikov N.A., Maksimova E.A., Alekseenko A.V. Designing modern living space: the model of risk-oriented safety evaluation at the level of physical access. Proceedings of Irkutsk State Technical University. 2016, vol. 20, no. 9, pp. 58–64. (In Russian) DOI: 10.21285/1814-3520-2016-9-58-64

Введение

Одним из показателей социальной доступности информационных систем и технологий в России является система современного жилого пространства «Умный дом» (УД). Это жилой дом современного типа, организованный для проживания людей при помощи автоматизации и высокотехнологичных устройств [1]. Под «умным домом» следует понимать информационную систему, которая обеспечивает безопасность, комфорт и ресурсосбережение для всех пользователей.

Как было отмечено авторами работы [2], система УД в России является привлекательной для злоумышленных воздействий. Следовательно, актуальной является задача обеспечения безопасности системы УД.

Риск-ориентированная оценка безопасности на уровне физического доступа

Существующие системы УД проектируются по следующим схемам [3]:

– централизованная – система, объединяющая все устройства с помощью центрального процессора;

– децентрализованная схема – система, в которой управление осуществляется через топологический элемент – шину, в пределах устройств;

– схема X10 – это схема построения протокола передачи управляющих сигналов (команд) по силовой электропроводке на электронные модули.

Данные схемы являются основополагающими в процессе проектирования системы защиты современного жилого пространства, так как позволяют определить уязвимые места, виды защищаемых элементов, структуру системы защиты и ее составляющие.

При создании системы защиты в системе УД возможно рассмотрение различных вариантов построения модели угроз [4]. В ходе исследования разработано дерево угроз безопасности системы УД (рис. 1), где U_i – возможные угрозы; U_1 – несанкционированное управление системой УД через Интернет; U_2 – кража информации через облачные системы; U_3 – перехват радиосигнала; U_4 – несанкционированное воздействие на систему УД побочными радиосигналами; U_5 – потеря пульта; U_6 – вывод из строя аппаратуры; U_7 – атака на сервер; U_8 – несанкционированное управление системой УД; U_9 – скачки напряжения; U_{10} – обесточивание дома; U_{11} – атаки на сервер X_{10}; U_{12} – побочные электромагнитные излучения; U_{13} – несанкционированное управление системой УД по радиоканалу в силовой проводке; U_{14} – наводки; U_{15} – вывод из строя оборудования; U_{16} – несанкционированное подключение к сети УД; U_{17} – конфликтное функционирование оборудова-

ния; U_{18} – ошибки пользователя; U_{19} – несанкционированный доступ (НСД) в помещение системы УД; U_{20} – НСД к центральной панели управления; U_{21} – НСД доступ к серверу системы УД; U_{22} – вывод из строя операционной системы[4].

При построении системы защиты решаются, в том числе, вопросы ее оптимизации. Одно из средств решения данной задачи связано с процессом зонирования жилого пространства. При выполнении зонирования современного жилого пространства с привязкой к дереву угроз в ходе исследования определена угроза на уровне физического доступа – доступ в помещение системы УД (рис. 2).

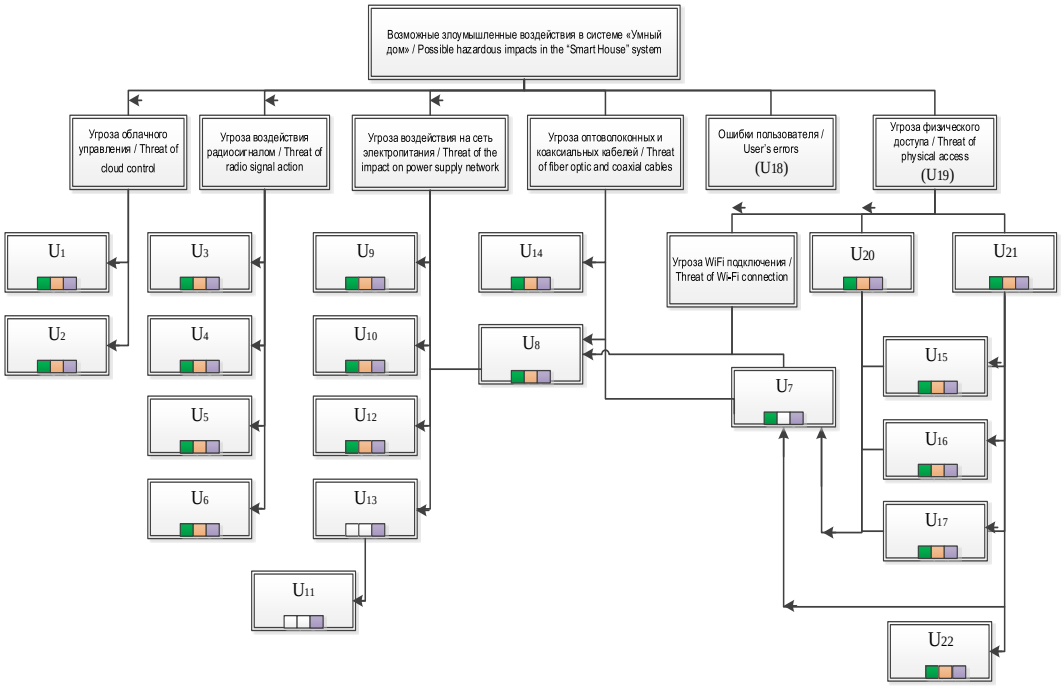


Рис. 1. Дерево угроз безопасности в системе УД
Fig. 1. Tree of security threats in the "Smart Home" system

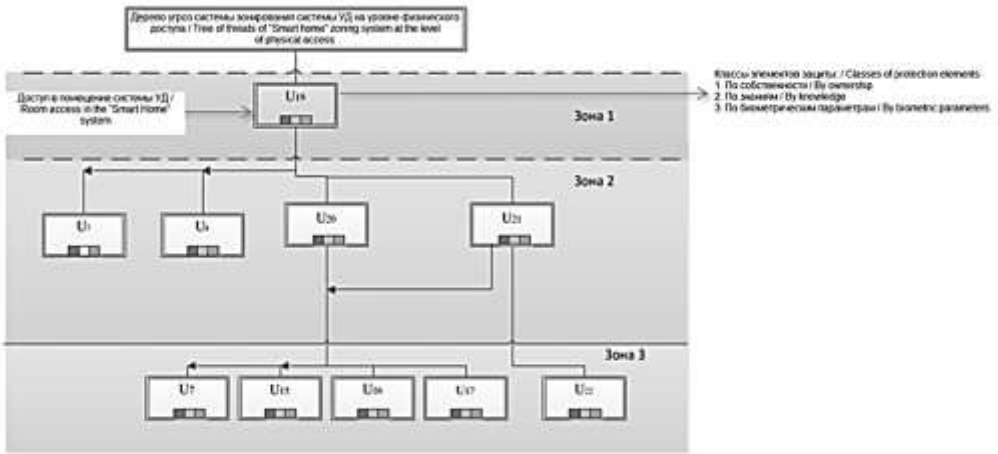


Рис. 2. Дерево угроз при зонировании системы УД
Fig. 2. Tree of threats under "Smart home" system zoning

[4]Перечень угроз представлен по ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (взамен ГОСТ 51275-96). М.: Стандартинформ, 2007. 11 с. / The list of threats is presented in accordance with the GOST P 51275-2006. Information protection. Informatization object. Factors influencing information. General Provisions (instead of GOST 51275-96). Moscow, Standartinform, 2007, 11 p.

Систематизация угроз в соответствии с зонированием позволяет говорить о приоритетности перекрытия угроз: максимальное перекрытие угроз первой зоны минимизирует риск проникновения во вторую и третью, следовательно, минимизирует требования к системе безопасности системы УД.

В первой зоне в качестве механизма защиты возможно использование элемента одного из классов – по собственности, по знаниям, по биометрическим параметрам[5]. Следовательно, задача сводится к выбору механизмов из данных классов, позволяющих минимизировать риски в системе защиты информации.

В системе УД предложена реализация модели риск-ориентированной оценки безопасности на уровне физического доступа. Элементами данной модели на количественном уровне являются вероятности реализации угрозы на уровне физического доступа. Изменение попыток идентификации – параметр влияния на данный показатель, оценить который возможно при помощи теории массового обслуживания.

В общем виде модель идентификации пользователя в системе УД представляется как однородная или неоднородная одноканальная система массового обслуживания с отказами без накопителя (рис. 3).

Разработанная графовая модель идентификации пользователя в системе УД представлена в виде модели массового обслуживания с дискретными состояниями и дискретным временем (рис. 4). В модели выделены следующие дискретные состояния:

– S_0 – начало входа в систему;
– S_1 – НСД выполнен успешно;
– S_2 – НСД выполнен неуспешно.

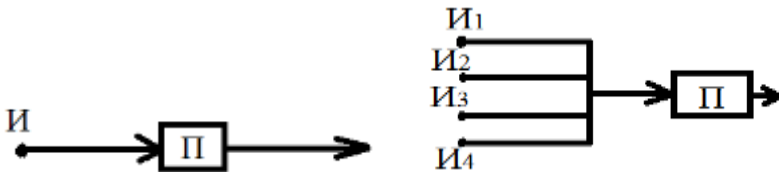
Для расчета вероятностей перехода системы из состояния S_i в состояние S_j (где $i = \overline{0,2}, j = \overline{0,2}$) после *n*-й попытки идентификации необходимо воспользоваться соответствующей матрицей перехода. Финальные вероятности состояний системы после *n*-й попытки идентификации $(P(0)^n)$ рассчитываются по формуле

$$P(0)^n = P(0) * \begin{pmatrix} P_6 & P_1 & P_2 \\ 0 & P_5 & 0 \\ 0 & P_4 & P_3 \end{pmatrix}^n,$$

где функция безопасности системы УД на уровне физического доступа в общем виде представима как

$$F = F(\{M_i\}, R),$$

где M_i – механизмы защиты системы УД; *R*– риски информационной безопасности.



а *б*

Рис. 3. Модель идентификации пользователя в системе УД: модели однородной (а) и неоднородной (б) одноканальной системы массового обслуживания с отказами без накопителя

Fig. 3. Model of user identification in the "Smart home" system: models of homogeneous (a) and heterogeneous (б) single-channel queuing system with refusals without a drive

[5]Прудник А.М., Власова Г.А., Рощупкин Я.В. Биометрические методы защиты информации: учеб.-метод. пособие. Минск: Изд-во БГУИР, 2014. 123 с. / Prudnik A.M., Vlasova G.A., Roshchupkin Y.V. Biometric methods of information protection: Learning and teaching aids. Minsk: BGUIR Publ., 2014, 123 p.

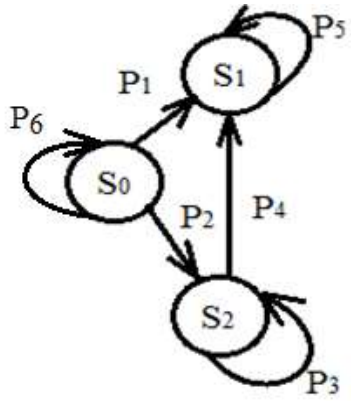


Рис. 4. Графовая модель идентификации пользователя в системе УД
Fig. 4. Graph model of user identification in the "Smart home" system

Механизмы защиты в свою очередь зависят от угрозы доступа в помещение системы УД. (U_{19}):

$$M_i = M_i(U).$$

Риск R представим в виде

$$R = R(\{P(0)^n{}_y\}, C),$$

где C – стоимость возможного ущерба от реализации соответствующей угрозы на уровне физического доступа; $P(0)^n{}_y$ – вероятности перехода системы из состояния S_i в состояние S_j.

В свою очередь

$$P(0)^n{}_2 = P(0)^n{}_2\ (P(0)^n{}_1);$$

$$P(0)^n{}_4 = P(0)^n{}_4\ (P(0)^n{}_3).$$

Тогда функция риска R имеет вид

$$R = R(P(0)^n{}_1, P(0)^n{}_3, P(0)^n{}_5, P(0)^n{}_6, C).$$

Таким образом, детализированная функция риск-ориентированной оценки безопасности системы УД на уровне физического доступа имеет вид

$$F = F\ (U, P(0)^n{}_1, P(0)^n{}_3, P(0)^n{}_5, P(0)^n{}_6, C).$$

Для определения максимального уровня риска безопасности системы УД рассчитывается значение возможного ущерба от реализации каждой угрозы при условии, что все $P^n{}_y$ = 1. В этом случае максимальный риск безопасности выглядит как

$$R_{max} = C.$$

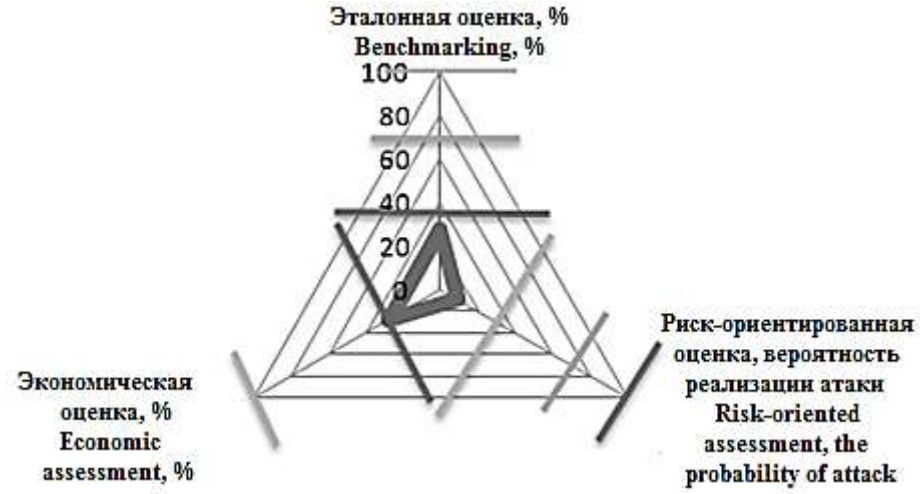
Уровень безопасности системы УД определяется в соответствии с границами, приведенными в таблице.

Предложенная модель реализована в программном комплексе «Оценка безопасности системы УД на уровне физического доступа» как часть интегральной оценки, учитывающей, в том числе, оценку по эталону и экономическим показателям [5].

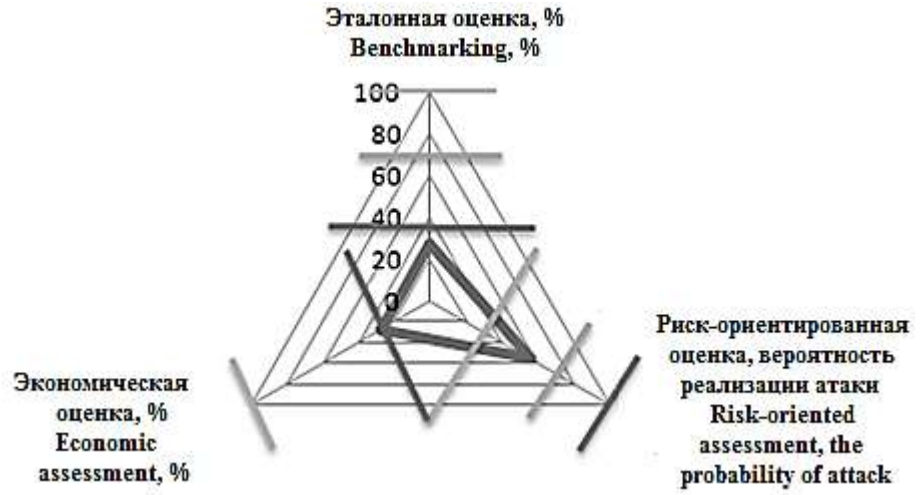
В ходе исследования проведена серия экспериментов при изменении параметров реализации атаки, количества попыток идентификации, изменении эталона. Результаты экспериментальных исследований по интегральной оценке для изменения значений риск-ориентированной оценки представлены на рис. 5.

Границы уровней безопасности системы УД на уровне физического доступа
Boundaries of the "Smart Home" system security levels at the physical access level

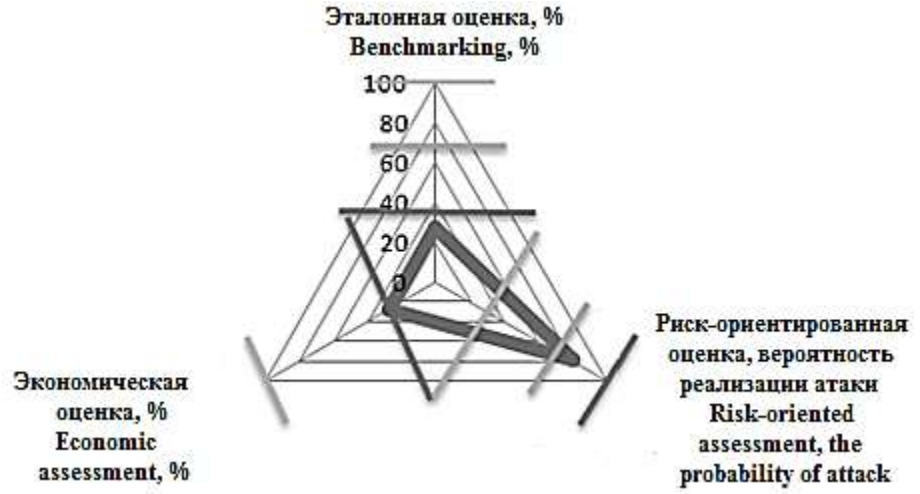
Уровень безопасности / Security level	Границы уровня безопасности / Boundaries of the security level
Высокий / High	[0–0,3 R_{max})
Средний / Medium	[0,3–0,6 R_{max})
Низкий / Low	[0,6–1 R_{max}]



а



б



в

Рис. 5. Результаты экспериментальных исследований по интегральной оценке безопасности системы УД на уровне физического доступа № 1 (а), № 2 (б), № 3 (в)
Fig. 5. Results of experimental studies on integrated safety evaluation of the "Smart home" system at the level of physical access no. 1 (a), no. 2 (b), no. 3 (c)

Выводы

По результатам риск-ориентированной, экономической и эталонной оценок находится интегральная оценка как сумма соответствующих баллов по каждой из обозначенных оценок и определяется общий уровень безопасности системы на уровне физического доступа.

Предложенная модель риск-ориентированной оценки безопасности системы УД на уровне физического доступа может использоваться как в локальном, так и в сетевом оценочном режиме, что позволяет достичь нового уровня эффективности проектного решения системы УД в целом.

Библиографический список

1. Умный дом [Электронный ресурс] // ВикипедиЯ. Свободная энциклопедия. URL: http://www.ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BC (04.03.2016).
2. Овчинников Н.А., Максимова Е.А. Разработка модели угроз системы защиты информации «умный дом» // Информационные системы и технологии. 2015. № 6 (92). С. 141–146.
3. Обзор систем и технологий «Умный дом» [Электронный ресурс] // Строительный ресурс. URL: http://forum.stroymart.com.ua/viewtopic.php?f=22&start=0&t=4928&view=print (04.03.2016).
4. Овчинников Н.А., Мисюрина К.В., Рудикова М.Н., Максимова Е.А. Формализованная модель информационной безопасности системы «Умный дом» // Апробация. 2016. № 1 (40). С. 49–51.
5. Программный комплекс «Исследование модели безопасности системы «Умный дом» с использованием биометрических средств защиты» / Н.А. Овчинников, Е.А. Максимова. Свидетельство о государственной регистрации № 2016614708. Правообладатель ФГАОУ ВО «Волгоградский государственный университет»; дата поступления 01.03.2016, дата гос. регистрации в Реестре программ для ЭВМ 28.04.2016.

References

1. Umnyi dom [Smart home]. Available at: http://www.ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BC (accessed 4 March 2016).
2. Ovchinnikov N.A., Maksimova E.A. Razrabotka modeli ugroz sistemy zashchity informatsii “umnyi dom” [Development of the model of threats of the “Smart Home” information security system]. Informatsionnye sistemy i tekhnologii [Information systems and technologies]. 2015, no. 6 (92), pp. 141–146. (In Russian)
3. Obzor sistem i tekhnologii "Umnyi do"» [Review of the “Smart Home” systems and technologies]. Available at: http://forum.stroymart.com.ua/viewtopic.php?f=22&start=0&t=4928&view=print (accessed 4 March 2016).
4. Ovchinnikov N.A., Misyurina K.V., Rudikova M.N., Maksimova E.A. Formalizovannaya model' informatsionnoi bezopasnosti sistemy "Umnyi dom" [Formalized model of “Smart Home” information security system]. Aprobatsiya [Approbation]. 2016, no. 1 (40), pp. 49–51. (In Russian)
5. Ovchinnikov N.A. Maksimov E.A. Issledovanie modeli bezopasnosti sistemy “Umnyi dom” s ispol'zovaniem biometricheskikh sredstv zashchity [Studying the model of the “Smart Home” security system with the use of biometric protection]. Certificate of state registration no. 2016614708. 2016. Rightholder FGAOU IN “Volgograd State University”; submitted 1 March 2016, the date of the state registration in the Register of Computer Programs 28 April 2016.

Критерии авторства

Авторы заявляют о равном участии в получении и оформлении научных результатов.

Authorship criteria

The authors declare equal participation in obtaining and formalizing of scientific results.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Статья поступила 21.06.2016 г.

The article was received 21 June 2016