НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2017 Том 17 № 3 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2017 Vol. 17 No 3 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.056

ВЫЯВЛЕНИЕ АНОМАЛИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ СИСТЕМЫ «УМНЫЙ ДОМ»

А.В. Настека[a], А.Н. Канев[a], Е.Е. Бессонова[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: nasteka.av@gmail.com

Информация о статье
Поступила в редакцию 15.02.17, принята к печати 15.03.17
doi: 10.17586/2226-1494-2017-17-3-450-456
Язык статьи – русский

Ссылка для цитирования: Настека А.В., Канев А.Н., Бессонова Е.Е. Выявление аномалий в беспроводных сенсорных сетях системы «Умный дом» // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 3. С. 450–456. doi: 10.17586/2226-1494-2017-17-3-450-456

Аннотация

Предмет исследования. Рассмотрена проблема выявления аномалий в системах домашней автоматизации «Умный дом». Определены особенности существующих охранных сетей, а также необходимость выявления информационного и физического воздействия на датчики в целях обеспечения информационной безопасности. **Метод**. Для выявления аномалий предложено использование искусственной нейронной сети. Метод предполагает обработку данных о характеристиках устройств охранной сети для определения аномального поведения. Искусственная нейронная сеть предварительно обучается на выборке таких данных. В работе представлено описание средств для практической реализации предложенного метода. **Основные результаты.** Для проведения эксперимента создан сценарий, по которому модель системы «Умный дом» передает данные об информационных потоках в сети, а искусственная нейронная сеть выносит решения на основе предоставленных данных. Таким образом, для тестирования созданы обучающая и тестовая выборки. Аномалией считалось состояние, для которого результат работы искусственной нейронной сети составлял величину не менее 0,9. По результатам тестирования искусственной нейронной сетью выносилось решение о принадлежности текущего состояния узла сети к аномальному или обычному состоянию с точностью 91%. **Практическая значимость.** Предложенный метод может быть использован при разработке информационных и охранных систем, для которых выдвигается требование мониторинга отдельных подключенных устройств. Технология выявления аномалий исключает возможность незаметного нарушения конфиденциальности и целостности передаваемой информации.

Ключевые слова
информационная безопасность, автоматизация помещений, устройства автоматизации, искусственная нейронная сеть

Благодарности
Авторы благодарят кафедру безопасных информационных технологий Университета ИТМО за поддержку и финансирование данного исследования.

ANOMALY DETECTION IN WIRELESS SENSOR NETWORKS OF «SMART HOME» SYSTEM

A.V. Nasteka[a], A.N. Kanev[a], C.E. Bessonova[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: nasteka.av@gmail.com

Article info
Received 05.02.17, accepted 15.03.17
doi: 10.17586/2226-1494-2017-17-3-450-456
Article in Russian

For citation: Nasteka A.V., Kanev A.N., Bessonova C.E. Anomaly detection in wireless sensor networks of «smart home» system. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 3, pp. 450–456 (in Russian). doi: 10.17586/2226-1494-2017-17-3-450-456

Abstract

Subject of Research. The paper reviews the problem of anomaly detection in home automation systems. The authors define present security networks specificities and highlight the need of informational and physical impact detection on sensors aimed at information security. **Method.** Artificial neural network is proposed for anomaly detection. This method processes the data on characteristics of security network devices for anomalous behavior detection. The artificial neural network should be preliminarily trained on the data of that type. The implementation tools for the proposed method of anomaly detection are

described. **Main Results.** The scenario has been created for the experiment so that the model of «Smart home» system produces the data of network information streams and the artificial neural network makes decisions based on this data. As a result, the training and testing sets have been created. The anomaly has been considered to be a state with the artificial neural network result less than 0.9. Based on the test results the artificial neural network determines the network node state with 91% precision. **Practical Relevance.** The proposed method can be used in information and security systems when connected devices should be monitored. Anomaly detection technology excludes inconspicuous violation of information confidentiality and integrity.

Keywords
information security, room automation, automation device, artificial neural network

Acknowledgements
We thank the Chair of Secure Information Technologies of ITMO University for supporting and facilitating this research.

Введение

В настоящее время одной из основных гарантий сохранности имущества в домах и квартирах является установка различных систем сигнализации и вывод тревожного сигнала на пульты частных охранных предприятий. Правоохранительных органы используют встраиваемое оборудование для создания охранных сетей [1], представляющих собой комплекс узлов и датчиков для предупреждения и возможного предотвращения противоправных действий. При физическом проникновении или ином отслеживаемом действии (вскрытие двери и т.п.) со стороны нарушителя данные устройства успешно сообщают о нем [2]. Однако, если влияние идет непосредственно на датчик или узел охранной сети, они не имеют возможности контролировать и реагировать на внешние программные и физические воздействия, которые не вписываются в стандартную модель поведения нарушителей.

В связи с развитием комплексов домашней автоматизации («Умный дом») охранные устройства все чаще внедряются в существующую инфраструктуру, где становятся еще более уязвимыми элементами сети и подвержены стандартным атакам типа distributed denial of service (DDoS). Реализация таких атак приводит к возникновению аномалий в системе. Таким образом, задачей исследования является разработка программного комплекса для выявления аномалий системы «Умный дом».

Вместе с появлением систем домашней автоматизации появились их первые уязвимости, и начались исследования устройств и сенсоров [3–5]. В том числе был разработан национальный стандарт[1] по построению автоматизированных систем управления зданиями, однако вопрос информационной безопасности в нем затронут лишь поверхностно. В 2015 году B.B. Mario, W. Candid показали в своей работе серьезные проблемы безопасности в существующих коммерческих решениях системы «Умный дом» [6]. Данные исследования показывают, что при достаточных знаниях злоумышленник способен обойти существующие механизмы защиты и воздействовать на конечные устройства автоматизации.

В работе А.В. Стариковского [7] показаны уязвимости систем домашней автоматизации, а также возможные каналы проникновения в их внутреннюю инфраструктуру. Подробно рассмотрены элементы системы, которые подлежат защите. Предложен концепт программы самозащиты для выявления проблем безопасности.

Raja Jurdak вместе с коллегами [8] на примере простого сценария показал теоретические основы для выявления аномалий в беспроводных сенсорных сетях и предложил признаки, по которым можно выявить ненормальное состояние системы. Недостатком работы является отсутствие каких-либо практических примеров применения полученных сведений.

Практических результатов добилась команда Girik Pachauri [9], которая искала аномальное поведение в медицинском оборудовании (датчики давления, датчики кислорода и др.). Исследуемые элементы также включены в беспроводную сенсорную сеть, что предполагает возможность взлома и нарушения их работоспособности. Для выявления аномалий авторы предложили использовать несколько базовых методов машинного обучения. Лучший результаты показал алгоритм Random Forest.

Наравне с базовыми методами машинного обучения в настоящей работе предлагается рассмотреть возможности искусственной нейронной сети. Она более гибко настраивается и устойчива к шуму во входных данных, способна быстрее адаптироваться под решение новых задач (изменение топологии сети, набора признаков). В работе предложено для выявления аномалий в беспроводной сенсорной сети использовать искусственную нейронную сеть, основанную на сети Кохонена и многослойном перцептроне. На момент написания настоящей работы авторам не известны случаи применения искусственной нейронной сети для поиска аномалий в беспроводной сенсорной сети системы «Умный дом».

Выявление аномалий с помощью искусственной нейронной сети

Общая схема возможного воздействия на устройства системы «Умный дом» представляет собой две стороны: злоумышленник и атакуемые устройства (рис. 1).

[1] СТО НП «АВОК» 8.1.3-2007 Стандарт АВОК. Автоматизированные системы управления зданиями. Часть 3. Функции. Введ. 01.09.2007.

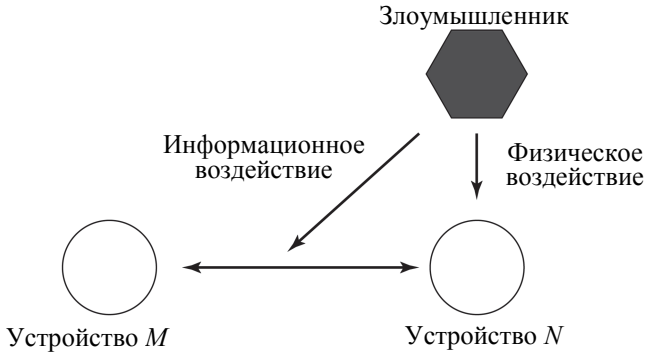

Рис. 1. Схема воздействия на устройства системы «Умный дом»

Злоумышленник имеет возможность физического вмешательства в работу устройства N (его отключение) [5, 6]. В этом случае устройством M может быть зарегистрирована аномалия в виде недоступного устройства N. Основным воздействием является информационное, которое направлено на информационный поток между устройствами N и M. Если устройством N ведется мониторинг активности сети, в частности, активность сетевого общения устройством M, то базовые атаки типа Man-in-the-middle, replay-атаки также приведут к образованию аномалий, которые злоумышленник не в состоянии скрыть [7].

Каждое из представленных выше воздействий тем или иным образом влияет на характеристики сети системы «Умный дом». Для решения поставленной задачи в первую очередь необходимо определить совокупность тех характеристик, которые будут анализироваться механизмом выявления аномалий (т.е. определить метрики).

Данные метрики различаются в зависимости от исследуемой аномалии [10]. В настоящей работе авторы выделили те из них, которые встречаются наиболее часто:

- количество входящих/исходящих пакетов за единицу времени;
- количество потерянных пакетов/ошибок за единицу времени;
- мощность исходящего сигнала;
- потребление электроэнергии за единицу времени.

Согласно [7], для выявления аномалий различного типа необходимо учитывать метрики соседних узлов сети. Также требуется хранить значения метрик в течение некоторого периода времени с целью выявления их изменений. Таким образом, каждый узел сети системы «Умный дом» можно представить как набор метрик, распределенных во времени.

Рассмотренный выше набор метрик является непостоянным и индивидуальным для конкретной реализации системы «Умный дом». Учитывая данные факторы, предлагается использовать машинное обучение как механизм обнаружения аномалий сети.

Машинное обучение включает в себя множество алгоритмов и методов для анализа данных. В случае задачи выявления аномалий в системе «Умный дом» необходимо на основе имеющихся значений определить каждое состояние как аномальное или нормальное. Так, в работе [9] авторами исследовано выявление аномалий в медицинском оборудовании с применением таких методов машинного обучения, как метод k ближайших соседей, дерево решений, random forest.

Искусственная нейронная сеть представляет собой математическую модель, построенную по примеру биологических нейронных сетей. За счет соединения относительно простых алгоритмов вместе и построения оптимальной связи между ними технология позволяет выявлять сложную зависимость между входными параметрами, даже если они изначально отсутствовали в обучающей выборке. Это позволяет алгоритму оставаться гибким при решении разного типа задач.

Авторами предложено использовать гибридную нейронную сеть, объединяющую две модели искусственных нейронных сетей: самоорганизующуюся сеть с конкуренцией (слой Кохонена) и многослойный персептрон [11]. Структура такой гибридной нейронной сети представлена на рис. 2. При этом полагается, что существует возможность выбрать иную структуру искусственной нейронной сети, с возможно лучшим показателем эффективности, однако эти результаты не вошли в предлагаемую работу.

Достоинством слоя Кохонена является высокая скорость обучения в сравнении с нейронными сетями с учителем. При заданной структуре он позволяет выделить наиболее важные входные данные (свойство локализации). Результирующий вектор передается на вход многослойному персептрону, функция которого состоит в определении, является ли переданный вектор аномальным или нет. В данном случае используется свойство аппроксимации персептронной сети.

Обучение гибридной сети проводится в несколько этапов: на первом обучается слой Кохонена, на втором – многослойный персептрон, при этом обучающая выборка подается через слой Кохонена. Методом обучения персептрона является метод обратного распространения ошибки [9].

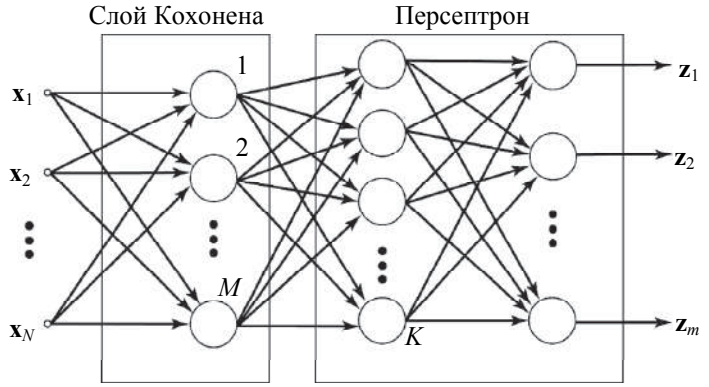

Рис. 2. Структура гибридной нейронной сети. На вход слоя Кохонена из M нейронов поступает вектор ($\mathbf{x}_1$, $\mathbf{x}_2$, … $\mathbf{x}_N$). Выходные данные слоя Кохонена, в свою очередь, поступают на вход многослойного персептрона. Каждый слой персептрона может иметь различное количество нейронов. На рисунке приведен случай двухслойного персептрона с K нейронами на первом слое. Выходом нейронной сети является вектор ($\mathbf{z}_1$, $\mathbf{z}_2$, …, $\mathbf{z}_m$)

В описанной выше модели используются следующие соотношения.

Значение каждого нейрона в слое Кохонена:

$$u_i = \sum_j w_{ji} x_j ,$$

где w_{ji} – вес связи i-го нейрона с j-м входом; x_j – j-й вход.

В слое выбирается «победитель»: $u_{\max} = \max\{u_i\}$, где $u_{\max}$ – «победитель». При этом используется механизм утомления для активации «мертвых» нейронов [2].

i-й выход слоя Кохонена:

$$y_i = \exp\left(-\frac{|u_{\max} - u_i|^2}{\sigma^2}\right),$$

где σ – подбираемое значение.

В ходе обучения слоя Кохонена веса «победителя» корректируются:

$$w_{ji} = w_{ji} + \alpha(x_j - w_{ji}),$$

где α – скорость обучения.

Значение i-го нейрона в k-м слое нейронов в персептроне:

$$z_i^{(k)} = \sum_j w_{ji}^{(k)} y_j^{(k-1)},$$

где $w_{ji}^{(k)}$ – вес связи i-го нейрона k-го слоя с j-м нейроном (k–1)-го слоя; $y_j^{(k-1)}$ – значение j-го нейрона в (k–1)-м слое; $k = 0$ – вход.

Практические результаты

Для практической реализации предложенного решения разработано два самостоятельных модуля, которые в дальнейшем объединятся в единую систему по выявлению аномалий в системе «Умный дом».

Первый модуль программно реализует искусственную нейронную сеть на языке C++. Он полностью повторяет представленную модель искусственной нейронной сети. В соответствии с описанной моделью выполняется обучение искусственной нейронной сети:

1. обучение слоя Кохонена;
2. обучение сети персептрона;

После обучения искусственная нейронная сеть готова к работе и способна на основании входящих данных выносить решения о принадлежности текущего состояния узла сети к аномальному.

Второй модуль реализует модели системы «Умный дом» в специальной среде моделирования (рис. 3). Для разработки этого модуля использовалась интегрированная среда (IDE) OMNeT++. OMNeT++ – объектно-ориентированный модульный фреймворк для симуляции событий сети. OMNeT++ позволяет моделировать беспроводные и проводные сети, протоколы их работы, имеет возможность встраивания пользовательских модулей на языке C++ [12]. С ее помощью смоделирована сеть с сенсорами, которые генерируют определенный поток трафика за единицу времени. Информация о трафике поступает на вход в искусственную нейронную сеть.

Оценка эффективности искусственной нейронной сети выполнена на основе следующего эксперимента. Создан сценарий, по которому модель системы «Умный дом» представляет данные об информационных потоках в сети, а искусственная нейронная сеть выносит решения на основе предоставленных данных. Основа экспериментальной модели – сценарий – включает в себя следующие элементы:

1. жилые помещения или автоматизированные помещения с сетью из датчиков общего назначения (датчики света, влажности и т.д.) и критически важных устройств (датчики пожарной и охранной сигнализации, датчики движения и т.д.);

2. злоумышленник с необходимыми знаниями и средствами для атаки;
3. устройство с искусственной нейронной сетью (УУ).

В определенный момент злоумышленник подключается к датчику температуры (АУ), и его действия создают дополнительное информационное воздействие.

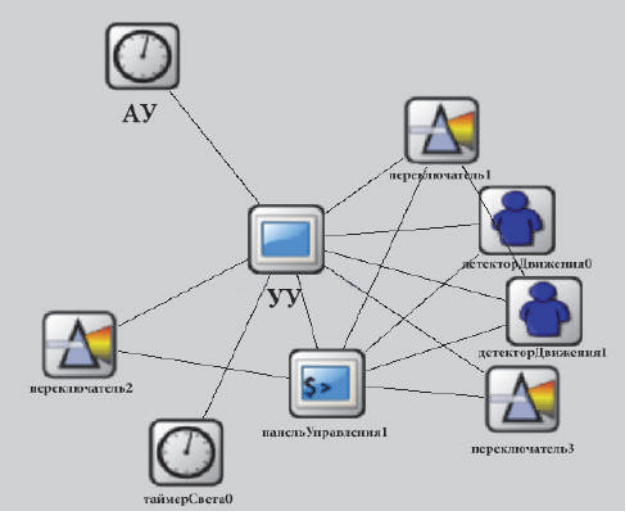

Рис. 3. Упрощенная модель системы «Умный дом» в IDE OMNeT++. Модель состоит из устройств системы «Умный дом», объединенных в сеть: устройство с искусственной нейронной сетью (УУ), датчик температуры, атакуемый злоумышленником (АУ), датчик света (таймерСвета0), датчики движения (детекторДвижения0, детекторДвижения1), переключатели (переключатель1, переключатель2, переключатель3), панель управления (панельУправления1)

В модели «Умный дом» использовано два ключевых устройства: УУ (устройство с детектором аномалий) и АУ (источник аномального трафика). Смоделирована ситуация, когда в трафик сети встраиваются дополнительные потоки данных, отсутствующие при нормальном режиме работы. Так, если опрос всех устройств с их данными (отправка запроса на получение пакета) проходит каждые 5 минут, то источник АУ начинает передавать случайным адресатам сообщения каждую минуту. Полученные данные позволяют провести анализ количества входящих пакетов за единицу времени на промежуточном узле УУ с помощью искусственной нейронной сети.

При информационном воздействии происходит изменение показателей трафика по сравнению с нормальным состоянием. В эксперименте в качестве входных данных использованы две метрики, наиболее показательные для выявления основных атак (DDoS): количество входящих пакетов за единицу времени и количество исходящих пакетов за единицу времени. Соответственно, размер входного вектора составляет 2 нейрона.

В ходе эксперимента протестированы несколько конфигураций искусственной нейронной сети. Качество конфигурации оценивалось на основе средней квадратичной ошибки. Итоговой является следующая конфигурация сети:

1. слой Кохонена: размер входного вектора – 2, количество нейронов в слое – 2; скорость обучения – 0,25;
2. персептрон: размер входного вектора – 2; количество слоев – 2; количество нейронов в каждом слое 10 и 5 соответственно; скорость обучения – 0,5.

Для тестирования созданы обучающая и тестовая выборки размером в 10000 каждая. В ходе эксперимента моделировалась ситуация, при которой периодически и кратковременно производилась передача данных от источника аномального трафика АУ. В тестовой выборке содержалось 118 аномальных состояний. Аномалией считалось состояние, для которой результат искусственной нейронной сети не ниже 0,9. Результаты обработки данных представлены в таблице.

Результат работы искусственной нейронной сети	Смоделированные состояния	
	Аномалия	Не аномалия
Аномалия	118	11
Не аномалия	0	9871

Таблица. Результаты эксперимента, количество состояний

Как показано в [13], в случаях, когда присутствует сильная асимметричность во входных данных, возможно использование полноты и точности для оценки эффективности классификатора. Точность показывает, какая часть выявленных объектов является релевантной. Полнота – это часть релевантных объектов, которые корректно выявлены. Показателем, представляющим собой среднее гармоническое точности и полноты, является *F*-мера. Максимум *F*-меры достигается при значениях точности и полноты в 100%. Соответственно, хороший классификатор должен пытаться достичь как можно более высокого значения *F*-меры [14]. Таким образом, для оценки эффективности работы искусственной нейронной сети использовались критерии:

– точность P
$$P = \frac{tp}{tp+fp} \times 100\%,$$
– полнота R
$$R = \frac{tp}{tp+fn} \times 100\%,$$
– сбалансированная *F*-мера:
$$F_1 = \frac{2 \times P \times R}{P+R} \times 100\%,$$

где *tp* – количество верно выявленных аномалий; *fp* – количество состояний, неверно оцененных искусственной нейронной сетью как аномалии; *fn* – количество состояний, неверно оцененных искусственной нейронной сетью как нормальные.

Эксперимент показал следующие результаты: $P = 91\%$, $R = 100\%$, $F_1 = 95\%$.

Следует отметить, что полученный результат *F*-меры не уступает результатам других методов машинного обучения при решении подобных задач [15]. Однако использование искусственной нейронной сети позволяет адаптироваться под новые условия рабочей среды. На практике это означает, что искусственная нейронная сеть может показать высокие значения показателей качества, в том числе на отличающихся от обучающей выборки входных данных. Отметим, что существует множество подходов (выбор топологии сети, методы обучения и т.д.), позволяющих оптимизировать искусственную нейронную сеть под конкретную задачу.

Заключение

В работе представлен алгоритм выявления аномалий сети системы «Умный дом» на основе искусственной нейронной сети. Научная новизна заключается в применении метода искусственной нейронной сети, ранее не используемого для поиска аномалий в беспроводных сенсорных сетях системы «Умный дом».

Предложенный метод поможет при разработке информационных и охранных систем, для которых выдвигается требование мониторинга отдельных подключенных устройств. Технология выявления аномалий исключит возможность незаметного нарушения конфиденциальности и целостности передаваемой информации с показателем сбалансированной *F*-меры 95%, что не уступает другим методам выявления аномалий с использованием машинного обучения.

На данный момент определена структура гибридной нейронной сети, а также описываются средства для практической реализации предложенного метода обнаружения аномалий. Определены метрики для выявления аномального состояния. В данной работе использовались две метрики: количество входящих пакетов за единицу времени; количество исходящих пакетов за единицу времени.

С помощью IDE Omnet++ создана модель беспроводной сенсорной сети, включающая в себя такие элементы, как сенсоры общего назначения, критически важные устройства, атакуемое устройство, устройство с искусственной нейронной сетью. В среде моделирования созданы рабочая и тестовая выборки данных размерностью 10000 каждая.

Дальнейшей работой авторов является проверка эффективности других метрик и оптимизация искусственной нейронной сети для повышения эффективности поиска аномалий.

Литература

1. Настека А.В., Бессонова Е.Е. Аутентификация устройств автоматизации в системе «Умный дом» // Вестник полиции. 2015. Т. 4. С. 68–74. doi: 10.13187/vesp.2015.4.68
2. Mafrur R., Khusumanegara P., Bang G.H., Lee D.K., Nugraha I.G.D., Choi D. Developing and evaluating mobile sensing for smart home control // International Journal of Smart Home. 2015. V. 9. N 3. P. 215–230. doi: 10.14257/ijsh.2015.9.3.20
3. Бессонова Е.Е., Ефремов А.А., Настека А.В.и др. Анализ защищенности систем «Умный дом» // Материалы конференции Региональная информатика «РИ-2014». Санкт-Петербург, 2014.
4. Pang Y., Jia S. Wireless smart home system based on Zigbee // International Journal of Smart Home. 2016. V. 10. N 4. P. 209–

References

1. Nasteka A.V., Bessonova E.E. Automation device authentication at «Smart Home». *Vestnik Policii*, 2015, vol. 4, no. 2, pp. 68–74. doi: 10.13187/vesp.2015.4.68 (In Russian)
2. Mafrur R., Khusumanegara P., Bang G.H., Lee D.K., Nugraha I.G.D., Choi D. Developing and evaluating mobile sensing for smart home control. *International Journal of Smart Home*, 2015, vol. 9, no. 3, pp. 215–230. doi: 10.14257/ijsh.2015.9.3.20
3. Bessonova E.E., Efremov A.A., Nasteka A.V. et. al. Security analysis of smart home system. *Proc. Conf. on Regional Informatics RI-2014*. St. Petersburg, 2014. (In Russian)
4. Pang Y., Jia S. Wireless smart home system based on Zigbee. *International Journal of Smart Home*, 2016, vol. 10, no. 4, pp. 209–220. doi: 10.14257/ijsh.2016.10.4.19

220. doi: 10.14257/ijsh.2016.10.4.19
5. Belaidouni S., Miraoui M., Tadj C. Towards an efficient smart space architecture // International Journal of Advanced Studies in Computer Science and Engineering. 2016. V. 5. N 1. P. 18–27.
6. Barcena M.B., Wueest C. Insecurity in the Internet of Things. Symantec, Report 21349619. 2015.
7. Стариковский А.В., Жуков И.Ю., Михайлов Д.М. и др. Исследование уязвимостей систем умного дома // Спецтехника и связь. 2012. №2. С. 55–57.
8. Jurdak R., Wang X.R., Obst O., Valencia P. Wireless sensor network anomalies: diagnosis and detection strategies // Intelligence-Based Systems Engineering. 2011. V. 10. P. 309–325. doi: 10.1007/978-3-642-17931-0_12
9. Pachauria G., Sharma S. Anomaly detection in medical wireless sensor networks using machine learning algorithms // Procedia Computer Science. 2015. V. 70. P. 325–333. doi: 10.1016/j.procs.2015.10.026
10. Son S.-Y. Home electricity consumption monitoring enhancement using smart device status information // International Journal of Smart Home. 2015. V 9. N 10. P. 189–196. doi: 10.14257/ijsh.2015.9.10.21
11. Осовский С. Нейронные сети для обработки информации. М.: Финансы и статистика, 2002. 344 с.
12. User Manual OMNeT++ version 4.6 [Электронный ресурс]. URL: https://omnetpp.org/doc/omnetpp/manual/usman.html.
13. Маннинг К.Д., Рагхаван П., Шютце Х. Введение в информационный поиск. М.: Вильямс, 2011. 528 с.
14. Bhattacharyya D.K., Kalita J.K. Network Anomaly Detection. A Machine Learning Perspective. CRC Press, 2014. 364 p.
15. Balagani K.S. K-Means+ID3 and Dependence Tree Methods for Supervised Anomaly Detection. PhD, Louisiana Tech University, 2008. 98 p.

5. Belaidouni S., Miraoui M., Tadj C. Towards an efficient smart space architecture. *International Journal of Advanced Studies in Computer Science and Engineering*, 2016, vol. 5, no. 1, pp. 18–27.
6. Barcena M.B., Wueest C. Insecurity in the Internet of Things. Symantec, *Report 21349619*, 2015.
7. Starikovskii A.V., Zhukov I.Yu., Mikhailov D.M. et. al. Vulnerability research of smart home systems. *Spetstekhnika i Svyaz'*, 2012, no. 2, pp. 55–57. (In Russian)
8. Jurdak R., Wang X.R., Obst O., Valencia P. Wireless sensor network anomalies: diagnosis and detection strategies. *Intelligence-Based Systems Engineering*, 2011, vol. 10, pp. 309–325. doi: 10.1007/978-3-642-17931-0_12
9. Pachauria G., Sharma S. Anomaly detection in medical wireless sensor networks using machine learning algorithms. *Procedia Computer Science*, 2015, vol. 70, pp. 325–333. doi: 10.1016/j.procs.2015.10.026
10. Son S.-Y. Home electricity consumption monitoring enhancement using smart device status information. *International Journal of Smart Home*, 2015, vol. 9, no. 10, pp. 189–196. doi: 10.14257/ijsh.2015.9.10.21
11. Osowski S. *Sieci Neuronowe do Przetwarzania Informacji*. Warszawa, 2000.
12. *User Manual OMNeT++ version 4.6*. Available at: https://omnetpp.org/doc/omnetpp/manual/usman.html.
13. Manning C.D., Raghavan P., Schutze H. *Introduction to Informational Retrieval*. Cambridge University Press, 2008, 504 p.
14. Bhattacharyya D.K., Kalita J.K. *Network Anomaly Detection. A Machine Learning Perspective*. CRC Press, 2014, 364 p.
15. Balagani K.S. *K-Means+ID3 and Dependence Tree Methods for Supervised Anomaly Detection*. PhD, Louisiana Tech University, 2008, 98 p.

Авторы

Настека Александр Владимирович – студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, nasteka.av@gmail.com

Канев Антон Николаевич – студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, kanev.a.n@mail.ru

Бессонова Екатерина Евгеньевна – кандидат технических наук, ассистент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, merom812@gmail.com

Authors

Alexander V. Nasteka – student, ITMO University, Saint Petersburg, 197101, Russian Federation, nasteka.av@gmail.com

Anton N. Kanev – student, ITMO University, Saint Petersburg, 197101, Russian Federation, kanev.a.n@mail.ru

Catherine E. Bessonova – PhD, Assistant, ITMO University, Saint Petersburg, 197101, Russian Federation, merom812@gmail.com