ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Сентябрь 2018 Том 6 № 3 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
September 2018 Vol. 6 Iss. 3 ISSN 2307-1303 http://www.itt.sut.ru

МОДЕЛИРОВАНИЕ И АНАЛИЗ АТАК ИСТОЩЕНИЯ ЭНЕРГОРЕСУРСОВ В СИСТЕМАХ ЦИФРОВОГО ГОРОДА

В. А. Десницкий[1*], Н. Н. Рудавин[1, 2]

[1] СПИИРАН, Санкт-Петербург, 199178, Российская Федерация
[2] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
* Адрес для переписки: desnitsky@comsec.spb.ru

Аннотация
Статья посвящена атакам истощения энергоресурсов систем Цифрового Города. **Предмет исследования.** Предметом исследования являются модели угроз информационной безопасности и нарушителя, осуществляющего атаки истощения энергоресурсов, в предметной области систем Цифрового Города. **Метод.** Применяются методы аналитического моделирования, а также анализ существующих работ в предметной области атак истощения ресурсов. **Основные результаты.** Проведен детальный анализ состояния исследований по направления атак истощения энергоресурсов, получен набор уязвимостей, связанных с истощением ресурсов систем Цифрового Города, а также построена единая модель нарушителя, выполняющего данный вид атак. **Практическая значимость.** Полученные в данной работе результаты могут применяться для совершенствования средств защиты киберфизических систем Цифрового Города от возможного вида атак истощения энергоресурсов автономно работающих устройств, участвующих в работе таких систем.

Ключевые слова
Цифровой Город, сенсорные сети, атаки истощения энергоресурсов.

Информация о статье
УДК 004.733
Язык статьи – русский.
Поступила в редакцию 01.08.18, принята к печати 03.09.18.

Ссылка для цитирования: Десницкий В. А., Рудавин Н. Н. Моделирование и анализ атак истощения энергоресурсов в системах цифрового города // Информационные технологии и телекоммуникации. 2018. Том 6. № 3. С. 10–18.

MODELING AND ANALYSIS OF ENERGY EXHAUSTION ATTACKS IN DIGITAL CITY SYSTEMS

V. Desnitsky[1*], N. Rudavin[1]

[1] SPIIRAS, St. Petersburg, 199178, Russian Federation
[2] ITMO University, St. Petersburg, 197101, Russian Federation
* Corresponding author: desnitsky@comsec.spb.ru

Abstract—The article is devoted to energy exhaustion attacks in Digital City systems. **Research subject.** The subject of the study is models of threats to information security and an intruder conducting energy exhaustion attacks of in the subject area of Digital City. **Method.** Methods of analytical modeling are applied as well as an analysis of existing work in the subject area of energy exhaustion attacks. **Core results.** A detailed analysis of the state of research in the field of the energy exhaustion, a set of vulnerabilities associated with the exhaustion of resources of the Digital City systems is formed, as well as a model of the intruder performing this type of attacks has been constructed. **Practical relevance.** The results obtained in this paper can be used to improve the means of protecting the cyber physical systems of the Digital City from the possible type of energy exhaustion attacks of autonomous de-vices involved in the operation of such systems.

Keywords—Digital City, sensor networks, energy exhaustion attacks.

Article info
Article in Russian.
Received 01.08.18, accepted 03.09.18.

For citation: Desnitsky V., Rudavin N.: Modeling and Analysis of Energy Exhaustion Attacks in Digital City Systems // Telecom IT. 2018. Vol. 6. Iss. 3. pp. 10–18 (in Russian).

Введение

Современные системы Цифрового Города представляют перспективную концепцию города, где цифровые технологии, в том числе и компоненты Интернета вещей, интегрированы в городскую среду для осуществления контроля и управления инфраструктурой города и городским имуществом, таким как системы энергоснабжения, дороги, образовательные и медицинские учреждения, органы местного самоуправления, а также другие государственные и коммерческие предприятия, находящиеся на территории города.

Важно понимать актуальность проблемы безопасности систем Цифрового Города с точки зрения защиты энергоресурсов таких систем по нескольким причинам. Во-первых, согласно программе «Цифровая экономика РФ» уже к 2025 г. на территории России предполагается создать 50 «умных городов». В рамках этого проекта предполагается развитие автономного транспорта, систем контроля объектов энергоснабжения и беспроводных точек доступа к Интернету. Во-вторых, концепция умного города подразумевает наличие множества автономных узлов сети, которые могут оказаться уязвимы, так как имеют беспроводной интерфейс. При этом часто возможен физический доступ к ним,

а низкое энергопотребление является важным условием их постоянной бесперебойной работы. В-третьих, в связи с ускоренными темпами развития и внедрения Интернета вещей, зачастую проявляются угрозы, для защиты от которых изначально не были предусмотрены контрмеры.

В статье демонстрируется возможность применения атак истощение энергоресурсов на устройства систем Цифрового Города. Также проведен анализ современных исследований, связанных с такими атаками для предметной области Цифрового Города. Помимо этого, статья содержит, как сведения о концепции Цифрового Города, так и возможные угрозы на элементы подобных систем.

Статья организована следующим образом: раздел 1 содержит обзор текущего состояния исследований; в разделе 2 приведены элементы концепции Цифрового Города в контексте атак истощения энергоресурсов; раздел 3 содержит анализ уязвимостей, которыми обладают системы Цифрового Города; раздел 4 раскрывает сущность и особенности модели нарушителя и угрозы, которые потенциальный нарушитель может эксплуатировать.

1 Обзор литературы

В настоящее время имеется множество работ, подтверждающих возможность реализации атак истощения энергоресурсов, а также их эффективность и возможность вывести из строя практически коммуникационную сеть даже при помощи одного устройства. В частности, реализация подобной атаки показана в [1]. В [2, 3, 4] раскрывается разновидность таких атак, называемая атака «отказ во сне» (*denial of sleep attack*), которая предотвращает запланированный переход устройства из режима полнофункциональной работы в режим ограниченного функционирования (сна) со сниженным энергопотреблением. Причем, как построены математические модели, основанные на случайных процессах, так и проведены эксперименты, в которых реализовывалась данная атака. Результаты экспериментов показали, насколько сильно влияют атаки типа denial-of-sleep на фактический расход энергоресурсов. В большинстве случает в качестве стартовой точки такие атаки используют беспроводной интерфейс сенсорных сетей. Как показано в [5, 6], атакующий производит атаку на протоколы транспортного уровня, вынуждая устройства производить обработку данных и не переключаться в режим низкого энергопотребления. Существует также множество решений по выявлению и принятию контрмер, противодействующих таким атакам. Например, в статье [3] предложено разделять элементы сенсорный сети на множество слоев, с целью недопущения влияния, атакующего на работу всей сети или зараженного некоторого узла. Также предлагается использовать модифицированные методы криптографии с распределением ключей для узлов подгрупп сенсорной сети, предотвращающие действия по вторжению в сеть с использованием атакующего узла [7]. В части атаки на конкретный узел, предлагаются решения, фильтрующие поток полезной информации и ложный, провоцирующий лишний выход и спящего режима [8, 9]. В целом проанализированные источники показывают резкое увеличение энергопотребления в процессе атак истощения энергоресурсов и незначительное увеличение (относительно нормального состояния) расхода заряда узлов в атакуемой сети в случае их эффективной защиты. Все эти работы подтверждает актуальность атак истощения энергоресурсов и их опасность применительно к сенсор-

ным сетям, а также необходимость применения эффективных средств обнаружения таких атак и противодействия.

2 Модель предметной области

Как и во всех проектах Интернета вещей важной особенностью концепции Цифрового Города является наличие множества автономных устройств, выполняющих отдельные задачи по сбору и обработке данных, а также выполнению действий на определенном участке. В совокупности эти устройства формируют сеть, которая выполняет задачи, в частности, по оптимизации управления и наблюдению за объектами инфраструктуры города [10].

В настоящее время рассматривается множество направлений цифровизации города: автономный городской транспорт, контроль экологической обстановки, системы электронного оповещения населения, городское видеонаблюдение, электронная медицина, проекты контроля энергоэффективности и проекты оптимизации дорожного движения. Причем, предполагается, что значительные количества таких устройств, а также, что расположены они могут быть в местах, труднодоступных для технических работников. Зачастую такие устройства/узлы могут размещаться в местах, отдаленных от систем электроснабжения и коммуникационных линий связи. Такие устройства производят беспроводную передачу данных и имеют автономный источник энергоснабжения (аккумулятор, либо портативную электростанцию).

Как правило, типовой узел можно разделить на несколько ключевых элементов:

1. Модуль связи беспроводной сети – как правило, использует сотовую связь, Wi-Fi либо другие протоколы сенсорных сетей;

2. Модуль-контроллер – он может быть разделен на верхний уровень, отвечающий за автономное выполнение задачи узла, и нижний уровень, получающий информацию с датчиков управляющий обратной связью;

3. Целевой модуль – видеокамера, GPS-модуль, RFID-метка, электромеханическое исполнительное устройство, а также другие специализированные под нужные задачи датчики и механизмы;

4. Элемент питания. Узлы могут быть подключены к общей системе энергоснабжения, но используются и полностью автономные узлы. В них элемент питания включает в себя аккумуляторную батарею с модулем заряда/разряда, контролирующем энергопотребление, а также при необходимости автономную мини-электростанцию.

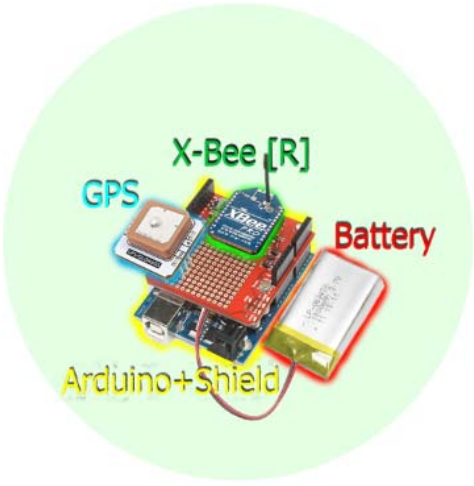

Рис. 1. Типовой элемент сенсорной сети

Примером такого модуля можно представить собранный в рамках построенного экспериментального стенда автономный узел, представленный на рис. 1. В его задачи входит передача сигнала сенсорной сети, а также отправка данных о своем местоположении в виде GPS-координат.

Здесь устройством беспроводной сети является модуль XBee S2, использующий протокол ZigBee. Особенность такой сети состоит в том, что обязательно наличие в сети координатора, а остальные устройства выполняют задачи маршрутизации либо осуществляют функции конечных (терминальных) устройств. Модуль-контроллер реализуется на аппаратной платформе Arduino Uno, который осуществляет обработку запросов от координатора и передачу данных о местоположении и других параметров узла. Также узел включает целевой модуль – датчик GPS neo5mv2 и элемент питания – литий-ионный аккумулятор 3,7 В емкостью 2,8 А. В последующих разделах приводится описание возможных угроз для подобных модулей сенсорных сетей, применяемых в проектах цифровизации городов.

3 Анализ угроз систем Цифрового Города

Рассмотрим основные возможные угрозы сенсорных сетей Цифрового Города и связанные с ними разновидности атак истощения энергоресурсов.

1. Пассивная атака на протоколы беспроводной передачи данных – прослушивание пакетов, посылаемых в соответствии с используемым протоколом маршрутизации. Получение информации о взаимодействии между узлами с выявлением их адресов, о примерном расположении узлов, о сетевой топологии. Непосредственной угрозой энергоресурсом такая уязвимость не является, однако нарушитель может перехватить пакеты, а после этого самостоятельно производить отправку пакетов реализуя, таким образом, атаку типа denial-of-sleep.

2. Перенаправление пакетов – использование протокола передачи данных и маршрутизации для перенаправления пакетов, идущих от или к целевому узлу, через определённый узел. При этом в сети начинают использоваться намеренно неоптимальные маршруты. Таким образом, злоумышленник имеет возможность, перехватывая пакеты, направлять их на определенный узел, который он хочет вывести из строя путем перерасхода энергии, вызванной постоянно нагруженной работой узла в роли маршрутизатора.

3. Программный отказ элемента – узел не предоставляет услуги другим, в том числе функции маршрутизации. Данная угроза может быть имплементирована программной ошибкой, в результате которой перестает действовать режим пониженного энергопотребления, или поступлением команды на отключение спящего режима элемента. Ресурсы при этом не потребляются выше расчетного, однако узел может перестать выполнять свои задачи, израсходовав энергоресурсы раньше расчетного времени.

4. Отбор энергетических ресурсов – вынуждая узел производить дополнительные действия, расходуется энергоресурс целевого узла, запасенного в источнике электропитания. Нарушитель, получив доступ к удаленному узлу, начинает тратить энергоресурсы в личных целях, также способствую досрочному разряду источника питания.

5. Активное обнаружение топологии сети – получение информации о сети, расположении элементов. Угроза может организовываться как отправкой маршрутных сообщений, позволяющих анализировать информацию об узлах и сети, так и визуальным обнаружением одного или нескольких элементов системы. Получив данные о сети и подключившись к наиболее уязвимому элементу, нарушитель имеет возможность произвести vampire-атаку [1] на всю сеть. Так-

же, как и в пассивной атаке на протокол маршрутизации, обнаружение может происходить удаленно сторонним нарушителем, однако уже с применением средств активного взаимодействия с сетью.

6. Атака типа «спуфинг» – атакующий узел выдает себя за узел сети определенной роли, в том числе роля координатора, получая возможность производить множество действий, в том числе функции управления сетью. В рамках этой угрозы предполагается именно наличие некоторого постороннего, выдающего себя за истинного участника, субъекта.

7. Зашумление канала связи (создание помех) – канал передачи данных заполняется посторонними шумами, которые могут иметь естественную (изменчивая среда передачи) и искусственную (постановщик активных/пассивных помех, либо загруженность частотного канала другими сетями) природу, вынуждая увеличивать узлами мощность антенны, а также вынуждая устройства многократно передавать пакеты данных ввиду потерь их.

8. Злонамеренная эксплуатация нарушителем открытого интерфейса устройства – имея физический доступ к системе или её части, возможно повреждение или уничтожение его элементов, а также подключение «паразитирующих» устройств, которые могут приводить к перерасходу энергоресурса, причем изначально малозаметному. Как правило, это связано с тем, что некоторые элементы системы, будучи универсальными и многозадачными, имеют открытые элементы интерфейса, как физического, так и сетевого, и через них возможно подключение нарушителя к устройству. Пример такой атаки показан на рис. 2.

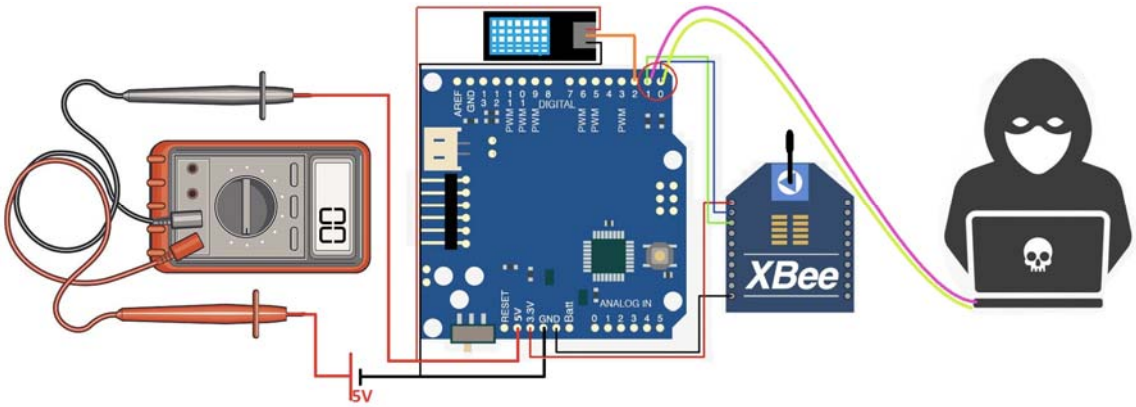

Рис. 2. Физическая реализация атаки на открытый интерфейс

Нарушитель подключился параллельно с датчиком X-Bee, тем самым зная основы работы протокола ZigBee, способен самостоятельно генерировать пакеты передачи данных для реализации vampire-атаки» [1], и вместе с тем нарушитель имеет возможность постоянно «пробуждать» узел сети, реализуя атаку типа denial-of-sleep.

4 Анализ нарушителя

Согласно большинству классификаций нарушитель может быть внешний либо внутренний в зависимости от возможности проникновения в защищенный периметр системы. Защищенным периметром является территория помещения с элементами системы, а также точки размещения узлов сети. Внутренний

нарушитель имеет физический доступ к элементам системы, тогда как внешний только к каналу передачи данных [11, 12].

Внешними нарушителями могут быть: 1) клиенты, пользователи; 2) представители конкурирующих организаций; 3) сотрудники органов ведомственного надзора и управления; 4) наблюдатели за пределами защищенного периметра.

Внутренними нарушителями могут быть: 1) операторы системы; 2) лица, ранее получившие несанкционированный доступ в систему.

Мотивы нарушителей могут быть следующие: 1) причинение имущественного ущерба путем мошенничества или иным преступным путем; 2) получение конкурентных преимуществ; 3) внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки; 4) любопытство или желание самореализации; 5) выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды; 6) реализация угроз безопасности информации из личных мотивов; 7) реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий; 8) несогласованная проверка надежности системы.

Могут использоваться следующие методы и принципы воздействия: 1) сбор информации и данных; 2) пассивные средства перехвата; 3) использование средств, входящих в информационную систему или систему ее защиты, и их недостатков; 4) активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок в систему, подключение к каналам передачи данных.

Таким образом, в таблице 1 приведены наиболее вероятные характеристики нарушителей для приведенных угроз безопасности. Используются следующие сокращения: «Вне 1-4» обозначены внешние нарушители, «Вну 1-2» – внутренние, «М 1-8» – мотивы, «В 1-4» – методы и принципы воздействия.

Таблица 1.

Моделирование нарушителей

Вид угрозы	Вид нарушителя	Мотив	Метод воздействия
1	Вне 2,3,4	М 2,4,5,8	В 1,2
2	Вну 1,2	М 1,3,5,6,8	В 3,4
3	Вне 1,2, Вну 1,2	М 1,4,5,7	В 3
4	Вне 3, Вну 2	М 2,3,6	В 1,3,4
5	Вне 1,2,3	М 2,4,5,8	В 1,2,4
6	Вне 1,2, Вну 2	М 1,4,6,8	В 3,4
7	Вне 2,3,4	М 2,4,6,8	В 4
8	Вне 2, Вну 1,2	М 1,3,4,7	В 1,3,4

Заключение

В работе раскрываются особенности концепции Цифрового Города применительно к задаче исследования атак истощения энергоресурсов, показана специфика данной предметной области, описаны типичные элементы сенсорных сетей систем, применяемых в рамках данной концепции, а также проведен обзор материалов, связанных с атаками истощения энергоресурсов на устройства Цифрового Города. Помимо этого, проведен анализ актуальных угроз систем Цифрового Города в контексте атак истощения энергоресурсов, а также представлена модель нарушителей, которые могли бы реализовать атаки. В дальнейшем планируется моделирование атак на физическом оборудовании Цифрового Города и получение их экспериментальных оценок с последующим формированием рекомендаций необходимых контрмер.

Работа выполнена при финансовой поддержке Гранта Президента Российской Федерации № МК-5848.2018.9.

Литература

1. Vasserman E. Y., Hopper N. Vampire attacks: draining life from wireless ad hoc sensor networks // IEEE transactions on mobile computing. 2013. Т. 12. № 2. pp. 318–332.

2. Shakhov V., Koo I. Depletion-of-Battery Attack: Specificity, Modelling and Analysis // Sensors. 2018. Т. 18. № 6. pp. 1849.

3. Bhattasali T., Chaki R., Sanyal S. Sleep deprivation attack detection in wireless sensor network // arXiv preprint arXiv:1203.0231. 2012.

4. Chen C. et al. An effective scheme for defending denial-of-sleep attack in wireless sensor networks // Information Assurance and Security, 2009. IAS'09. Fifth International Conference on. IEEE, 2009. Т. 2. pp. 446–449.

5. Jo M. et al. A survey: energy exhausting attacks in MAC protocols in WBANs // Telecommunication Systems. 2015. Т. 58. № 2. pp. 153–164.

6. Raymond D. R. et al. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols // IEEE transactions on vehicular technology. 2009. Т. 58. №. 1. pp. 367–380.

7. Hsueh C. T., Wen C. Y., Ouyang Y. C. A secure scheme against power exhausting attacks in hierarchical wireless sensor networks // IEEE Sensors journal. 2015. Т. 15. №. 6. pp. 3590–3602.

8. Hei X. et al. Defending resource depletion attacks on implantable medical devices // Global telecommunications conference (GLOBECOM 2010), 2010 IEEE. IEEE, 2010. pp. 1–5.

9. Guo Z. et al. An efficient approach to prevent Battery Exhaustion Attack on BLE-based mesh networks //Computing, Networking and Communications (ICNC), 2017 International Conference on. IEEE, 2017. pp. 1–5.

10. Jo M. et al. A survey: energy exhausting attacks in MAC protocols in WBANs // Telecommunication Systems. 2015. Т. 58. № 2. pp. 153–164

11. Desnitsky V., Kotenko I. Expert knowledge based design and verification of secure systems with embedded devices // Lecture Notes in Computer Science. 2014. Т. 8708. pp. 194–210.

12. Десницкий В. А., Котенко И. В. проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы. 2013. № 1. С. 44–54.

13. Десницкий В. А., Котенко И. В., Чечулин А. А. построение и тестирование безопасных встроенных систем // Труды XII Санкт-Петербургской международной конференции Региональная информатика (РИ-2010). 2011. С. 115–121.

References

1. Vasserman, E. Y., Hopper, N. Vampire attacks: draining life from wireless ad hoc sensor networks // IEEE transactions on mobile computing. 2013. T. 12. N. 2. pp. 318–332.

2. Shakhov, V., Koo, I. Depletion-of-Battery Attack: Specificity, Modelling and Analysis // Sensors. 2018. Vol. 18. N. 6. pp. 1849.

3. Bhattasali, T., Chaki, R., Sanyal, S. Sleep deprivation attack detection in wireless sensor network // arXiv preprint arXiv:1203.0231. 2012.

4. Chen, C. et al. An effective scheme for defending denial-of-sleep attack in wireless sensor networks //Information Assurance and Security, 2009. IAS'09. Fifth International Conference on. IEEE, 2009. Vol. 2. pp. 446–449.

5. Jo, M. et al. A survey: energy exhausting attacks in MAC protocols in WBANs // Telecommunication Systems. 2015. Vol. 58. N. 2. pp. 153–164.

6. Raymond, D. R. et al. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols //IEEE transactions on vehicular technology. 2009. Vol. 58. N. 1. pp. 367–380.

7. Hsueh, C. T., Wen, C. Y., Ouyang, Y. C. A secure scheme against power exhausting attacks in hierarchical wireless sensor networks // IEEE Sensors journal. 2015. Vol. 15. N. 6. pp. 3590–3602.

8. Hei, X. et al. Defending resource depletion attacks on implantable medical devices // Global telecommunications conference (GLOBECOM 2010), 2010 IEEE. 2010. pp. 1–5.

9. Guo, Z. et al. An efficient approach to prevent Battery Exhaustion Attack on BLE-based mesh networks // Computing, Networking and Communications (ICNC), 2017 International Conference on. IEEE, 2017. pp. 1–5.

10. Jo, M. et al. A survey: energy exhausting attacks in MAC protocols in WBANs // Telecommunication Systems. 2015. Vol. 58. N. 2. pp. 153–164.

11. Desnitsky, V., Kotenko, I. Expert knowledge based design and verification of secure systems with embedded devices // Lecture Notes in Computer Science. 2014. Vol. 8708. pp. 194–210.

12. Desnitsky, V., Kotenko, I. Designing of the protected built in devices on the basis of a configuration // Problems of information safety. Computer systems. 2013. No. 1. pp. 44–54.

13. Desnitsky, V., Kotenko, I., Chechulin, A. Construction and testing of secure embedded systems // Proceedings of the XII St. Petersburg International Conference Regional Informatics (RI-2010). 2011. pp. 115–121.

Десницкий Василий Алексеевич – кандидат технических наук,
старший научный сотрудник, СПИИРАН,
Санкт-Петербург, 199178, Российская Федерация,
desnitsky@comsec.spb.ru

Рудавин Николай Николаевич – программист, СПИИРАН, Санкт-Петербург, 199178;
студент магистратуры, Университет ИТМО,
Санкт-Петербург, 197101, Российская Федерация,
nikolay-rudavin@yandex.ru

Desnitsky Vasily – Candidate of Engineering Sciences,
Senior Research Officer, SPIIRAS, St. Petersburg,
199178, Russian Federation,
desnitsky@comsec.spb.ru

Rudavin Nikolay – Programmer, SPIIRAS, St. Petersburg, 199178;
Undergraduate, ITMO University, St. Petersburg,
197101, Russian Federation,
nikolay-rudavin@yandex.ru