НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2018 Том 18 №1 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2018 Vol. 18 No 1 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.021

ПОДХОД К КЛАССИФИКАЦИИ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕМЕНТОВ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

В.В. Семенов[a], И.С. Лебедев[a], М.Е. Сухопаров[b]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[b] Санкт-Петербургский филиал АО «НПК «ТРИСТАН», Санкт-Петербург, 195220, Российская Федерация
Адрес для переписки: semenov@corp.ifmo.ru

Информация о статье
Поступила в редакцию 23.11.17, принята к печати 28.12.17
doi: 10.17586/2226-1494-2018-18-1-98-105
Язык статьи – русский

Ссылка для цитирования: Семенов В.В., Лебедев И.С., Сухопаров М.Е. Подход к классификации состояния информационной безопасности элементов киберфизических систем с использованием побочного электромагнитного излучения // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 1. С. 98–105. doi: 10.17586/2226-1494-2018-18-1-98-105

Аннотация
Рассмотрены проблемные вопросы обеспечения информационной безопасности киберфизических систем. Проведен анализ характеристик автономных объектов. Представлена модель для системы мониторинга информационной безопасности, основанная на характеристиках, получаемых в результате анализа электромагнитного излучения электронных компонент автономных устройств киберфизических систем. Показана типовая схема определения состояния системы. Ввиду особенностей устройств, обеспечивающих инфраструктуру, оценивание состояния информационной безопасности направлено на анализ нормального функционирования системы, а не на поиск сигнатур и характеристик аномалий при проведении различного рода информационных атак. Раскрыт эксперимент, обеспечивающий получение статистической информации о работе удаленных устройств киберфизических систем, где накопление данных для принятия решения происходит путем сравнения статистической информации. Представлены результаты эксперимента по информационному воздействию на типовую систему. Предложенный подход анализа статистических данных автономных устройств на основе наивного байесовского классификатора может быть использован для определения состояний информационной безопасности. Особенностью подхода является возможность быстрой адаптации и применения различного математического аппарата, методов машинного обучения для достижения заданного качества вероятностной оценки состояния информационной безопасности. Реализация данного вида мониторинга не требует разработки сложных системных приложений, позволяет реализовывать различные архитектуры построения систем, производящие обработку на борту автономного объекта либо передачу данных и вычисление состояния на внешних вычислительных узлах систем мониторинга и контроля.

Ключевые слова
информационная безопасность, киберфизические системы, системы мониторинга информационной безопасности

APPROACH TO CLASSIFICATION OF THE INFORMATION SECURITY STATE OF ELEMENTS FOR CYBER-PHYSICAL SYSTEMS BY APPLYING SIDE ELECTROMAGNETIC RADIATION

V.V. Semenov[a], I.S. Lebedev[a], M.E. Sukhoparov[b]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
[b] Saint Petersburg Branch AO «NPK «TRISTAN», Saint Petersburg, 195220, Russian Federation
Corresponding author: semenov@corp.ifmo.ru

Article info
Received 23.11.17, accepted 28.12.17
doi: 10.17586/2226-1494-2018-18-1-98-105
Article in Russian

For citation: Semenov V.V., Lebedev I.S., Sukhoparov M.E. Approach to classification of the information security state of elements for cyber-physical systems by applying side electromagnetic radiation. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 1, pp. 98–105 (in Russian). doi: 10.17586/2226-1494-2018-18-1-98-105

Abstract
We consider problematic issues of information security for cyber-physical systems. The analysis of the characteristics of autonomous objects has been carried out. The paper presents a model for the information security monitoring system based on the characteristics obtained as a result of the electromagnetic radiation analysis of the electronic components of the autonomous devices in cyber-physical systems. A typical scheme for the system state determination is shown. For reasons of the device features providing the infrastructure, information security state assessment is aimed at the analysis of the system normal functioning, rather than the search for signatures and characteristics of anomalies during various types of information attacks. An experiment is described providing statistical information on the operation of remote devices of cyber-physical systems where data accumulation for decision-making occurs by statistical information comparison. The experiment results on information impact on a typical system are presented. The proposed approach for the statistical data analysis of autonomous devices based on a naive Bayesian classifier can be used to determine the information security states. A special feature of our approach is the ability for quick adaptation and application of various mathematical apparatus, and machine learning methods to achieve given quality of probabilistic assessment of information security state. The implementation of this type of monitoring does not require the development of complex system applications. It allows for implementation of various system building architectures processing the autonomous object on-board or data transfer and state calculation on external computer nodes of monitoring and control systems.

Keywords
information security, cyber-physical systems, information security monitoring systems

Введение

Современный этап развития киберфизических систем (КФС) характеризуется применением беспилотных средств – летающих объектов, автомобилей, поездов. Отсутствие оператора или наличие только удаленного контроля обусловливает возможность информационного воздействия на них вне контролируемой зоны, делает подобные средства очень привлекательной мишенью для попыток проведения различного рода атак [1–3]. Реализация большого числа проектов, связанных с беспилотными системами, вызывает необходимость обеспечения требуемого уровня безопасности циркулирующих в них данных.

Внедрение беспилотных средств сопровождается дополнительными проблемными вопросами обеспечения информационной безопасности, в том числе [4, 5]:

- обнаружение несанкционированного доступа к основным узлам на программном уровне;
- анализ и выявление аномалий в технологических циклах функционирования беспилотного средства;
- обнаружение деструктивного информационного воздействия на программы и алгоритмы;
- контроль версий программного обеспечения на предмет обнаружения недекларированных возможностей.

Выявление аномальных параметров функционирования, отклонений различных характеристик, неправильных или не соответствующих установленной ситуации команд, большого числа повторных событий, является важной задачей для обеспечения информационной безопасности КФС [6–8].

Дополнительные средства защиты потребляют информационные, энергетические ресурсы, имеют габариты и весовые характеристики, что в условиях ограничений беспилотных аппаратов не всегда приемлемо, а в случае несанкционированного доступа и модификации кода программного обеспечения они могут потерять свою эффективность. В связи с этим возникает ряд задач, направленных на осуществление внешнего мониторинга событий информационной безопасности объектов.

Постановка задачи

Эффективные решения в области информационной безопасности связаны с развитием научно-методического аппарата, направленного на повышение качественных показателей идентификации состояния защищенности, вследствие чего возникает необходимость разработки моделей и методов мониторинга информационной безопасности автономных вычислительных средств [9, 10], учитывающих особенности КФС.

Одним из подходов может быть использование электромагнитного излучения различных функционирующих электронных компонент. Для выявления аномального поведения необходимо использовать характеристики, отражающие состояния системы, которые могут быть применены в статистическом анализе [11]. В рассматриваемом случае контролирующая система D состоит из множества датчиков $\{d_1, d_2, \dots, d_n\}$, которые снимают излучаемые сигналы с компонент устройства. Каждый элемент системы d_i обрабатывает сигнал $s_{di}(t)$ от компоненты, где он расположен. В результате преобразований в моменты времени $t = 0,1\dots m$ от датчика d_i появляется последовательность значений $\{s_{di}(0), s_{di}(1),..., s_{di}(m)\}$. Синхронизируя по времени процесс съема значений элементов $\{d_1, d_2, \dots, d_n\}$ получаем в моменты времени $t = 0, 1, \dots, m$ кортежи характеристик $\{s_{d1}(0), s_{d2}(0),..., s_{dn}(0)\}$, $\{s_{d1}(1), s_{d2}(1),..., s_{dn}(1)\},\dots$, $\{s_{d1}(m), s_{d2}(m),..., s_{dn}(m)\}$.

Допустив, что от датчиков, расположенных на разных компонентах, где протекают программные процессы, в один момент времени можно получить набор значений признаков, задачу определения состояния информационной безопасности можно свести к задаче классификации.

Предлагаемый подход

Поведение системы в динамике предполагает, что переходы из состояния в состояние могут происходить в любой момент времени. Накопление данных для обучающей выборки происходит в зависимости от получаемых амплитудно-частотных значений излучений электронных компонент в различных режимах работы, определяемых составом запущенного программного обеспечения. В ходе накопления данных наблюдается изменение статистического портрета электромагнитного излучения функционирования устройств. Основу модели профиля исследуемого объекта составляют сигналы $s_{di}(t)$, излучаемые от разных элементов схем, как последовательность значений $\{s_{di}(0), s_{di}(1),..., s_{di}(m)\}$. Множество сигналов контролирующей системы D создают кортеж значений сигналов от различных датчиков по времени:

$$D(s_{di}(t),t)=\begin{vmatrix} s_{d1}(0) & s_{d1}(1) & ... & s_{d1}(m) \\ s_{d2}(0) & s_{d2}(1) & ... & s_{d2}(m) \\ ... & ... & ... & ... \\ s_{dn}(0) & s_{dn}(1) & ... & s_{dn}(m) \end{vmatrix}. \quad (1)$$

Представление данных в виде (1) позволяет применить различные методы машинного обучения для реализации классификатора. Исходя из этого, идентификацию состояния возможно осуществить на основе наивного байесовского классификатора (НБК), достоинством которого является малое количество данных для обучения:

$$C=\arg\max_{c} \; p(C=c)\prod_{i=1}^{n} p(D(s_{di}(\dot{t}),\dot{t})=\dot{d}_i \,|\, C=c), \quad (2)$$

где C – множество, описывающее возможные состояния системы; c – определенное состояние системы («нормальное» или «аномальное»); $\dot{t}$ – дискретный момент времени; $s_{di}(\dot{t})$ – значение сигнала от датчика d_i в момент времени $\dot{t}$; $D(s_{di}(\dot{t}),\dot{t})$ – кортеж значений сигналов от различных датчиков по времени $\dot{t}$.

Обрабатывая посредством НБК кортеж признаков, полученный через постоянные заданные промежутки времени, можно определить аномальные состояния системы, на которые следует обратить более пристальное внимание.

Эксперимент

С учетом того, что в ряде задач необходимо осуществление внешнего независимого мониторинга [11], в данной работе в качестве источника информации о состоянии рассматриваются побочные электромагнитные излучения и наводки (ПЭМИН) от средств вычислительной техники, возникающие при функционировании электронных устройств.

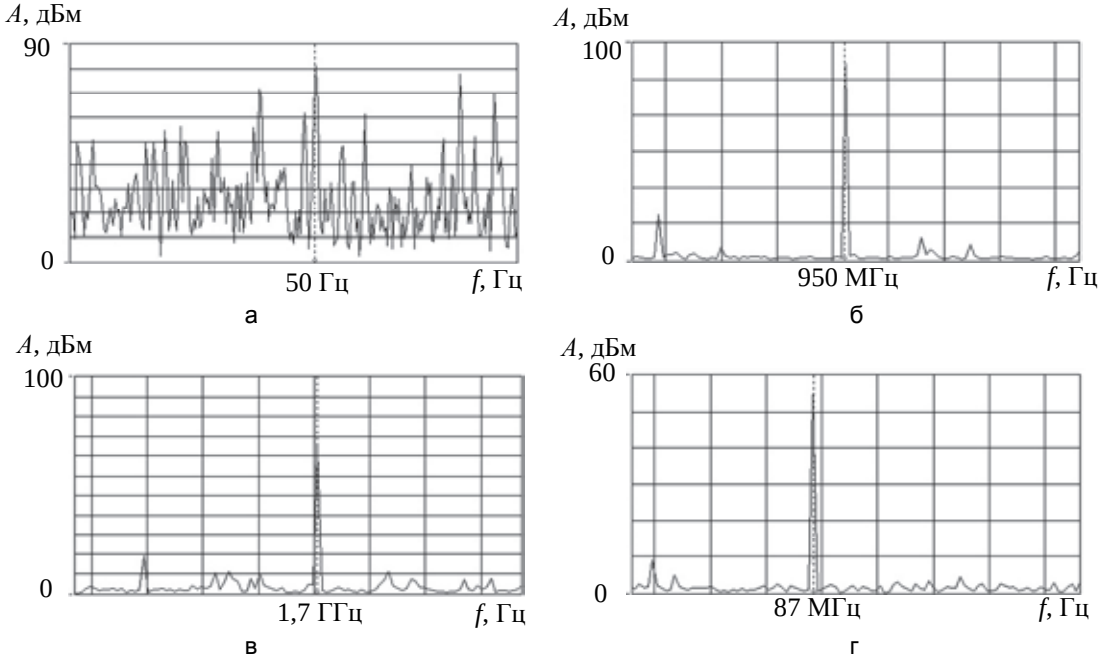


Рис. 1. Исследуемые пики сигналов для: датчиков типа АП Е3-50 (а); зондов ближнего поля типа NFP-3-P1 (б); зондов ближнего поля типа NFP-3-P2 (в); зондов ближнего поля типа NFP-3-P3 (г)

Измерения ПЭМИН показывают лучшие результаты в безэховых экранированных камерах, однако они не всегда доступны разработчикам и сложно применимы в полевых условиях. При проведении экс-

перимента допускалось, что при развертывании системы имеется некоторый временной интервал, на котором можно снять текущие параметры электромагнитного излучения, до момента деструктивного воздействия со стороны потенциального злоумышленника.

Измерения проводились на различных частотах несколькими датчиками одновременно от 50 Гц до 4 ГГц для разных элементов. Выбор наиболее информативных частот производился оператором. На более высоких частотах (f) приоритет отдавался значениям с наибольшей амплитудой (A) обратной связи. На рис. 1 представлены исследуемые пики.

На рис. 2 представлена схема проведения эксперимента. Каждый датчик исследуемого вычислительного блока соединен с анализатором спектра. Информация от датчиков оцифровывалась, накапливалась и синхронизировалась по времени, затем формировались кортежи матрицы (1), которые анализировались с помощью решающего правила на основе наивного байесовского классификатора (2).

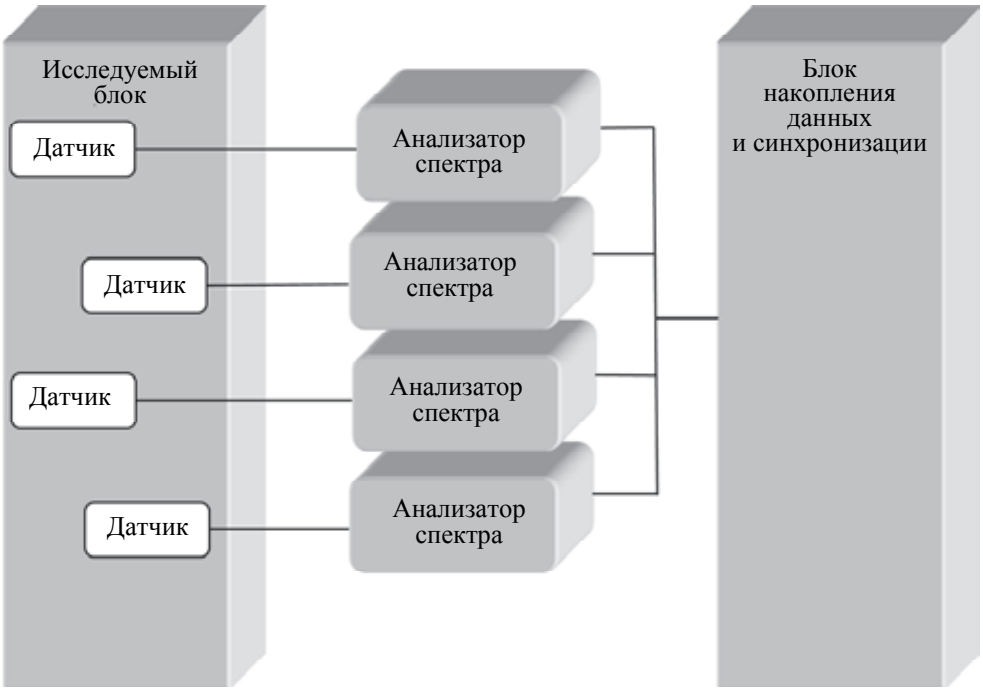
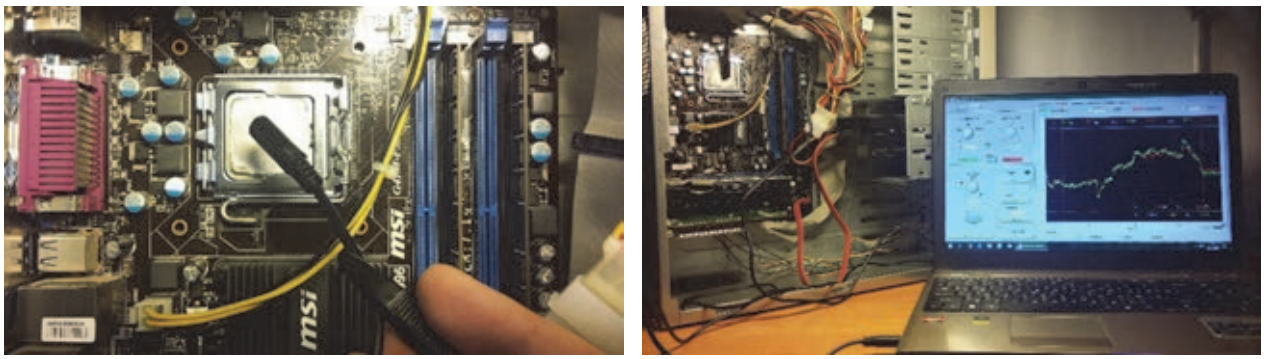


Рис. 2. Схема стенда проведения эксперимента

Для анализа и обработки использовался профиль, где накапливались, хранились параметры внешних поведенческих признаков, снимаемых с датчиков, для каждой совокупности процессов.

В качестве нормального состояния был выбран процесс, запущенный на операционной системе и выполняющий в вечном цикле операции умножения, деления и вывода результата на консоль. В качестве аномального состояния для анализа и сравнения рассматривались характеристики, когда вместо первого процесса запускался процесс, осуществляющий в вечном цикле только печать (вывод) символа на консоль без дополнительных вычислений.

В проведенном эксперименте электромагнитное излучение снималось над узловыми микросхемами материнской платы MSI G41M-P33 Combo (рис. 3).



а б

Рис. 3. Датчики над поверхностью процессора (а) и установка для измерения (б)

Полученные данные оцифровывались, и над ними производился анализ на основе НБК. В рассматриваемом случае будем считать, что множество классов C принимает значения $C = \{c_0, c_1\}$, c_0 – безопасное состояние, где функционируют только заранее разрешенные процессы, c_1 – небезопасное состояние, в котором произведен запуск «измененного» или несанкционированного процесса.

На графиках (рис. 4, 5) представлены значения амплитуд сигналов с шагом 500 мс для полученных данных разных тестовых программ с датчиков, установленных рядом с узловыми микросхемами.

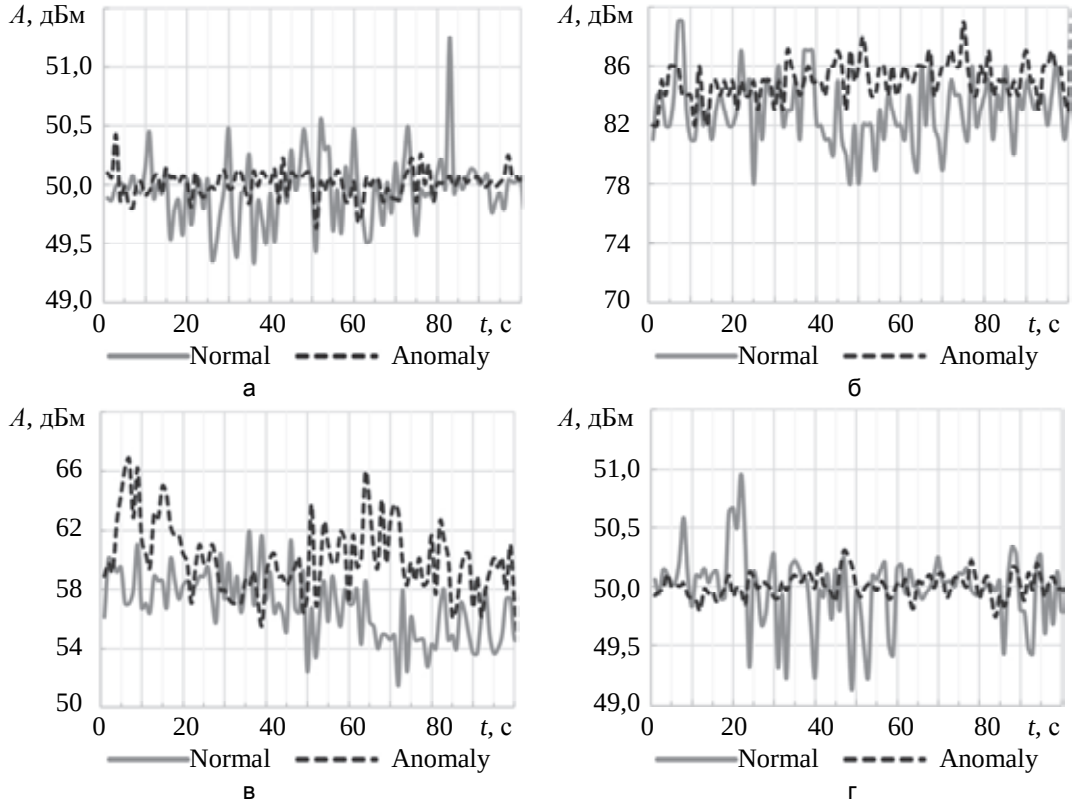


Рис. 4. Вид графиков колебаний амплитуды исследуемых пиков сигналов при нормальном функционировании системы и аномальном в случае непосредственного расположения датчиков над поверхностью микросхемы для: датчиков типа АП Е3-50 (а); зондов ближнего поля типа NFP-3-P1 (б); зондов ближнего поля типа NFP-3-P2 (в); зондов ближнего поля типа NFP-3-P3 (г). Normal – «нормальное состояние», Anomaly – «аномальное состояние»

Во время проведения эксперимента некоторые значения оказываются зашумленными, и по показанию ряда датчиков сложно определить состояние, однако оцифрованные значения от одновременного съема информации на кратковременном этапе дают возможность произвести оценку состояния в простейшей бинарной классификации.

С учетом специфики изделий, применяемых для автономных объектов киберфизических систем, одним из проблемных вопросов является расположение элементов, позволяющих получить исходные для анализа данные. В некоторых случаях невозможно организовать соприкосновение системы мониторинга с поверхностью, поэтому возникает необходимость вероятностной оценки определения состояния системы на различных расстояниях датчиков. Увеличивая или уменьшая расстояние, а также углы наклона от узловых микросхем поверхности съема датчиков, получаем изменение портретов сигналов (рис. 5).

Представленные на рис. 4, 5 для каждого эксперимента по отдельности графики преобразуются в кортежи значений сигналов D от различных датчиков по времени. Вероятность нахождения исследуемой системы в опасном или безопасном состоянии определяется на основе формулы (2).

Проведенный эксперимент показал, что с учетом «зашумленности» информации, получаемой от датчиков, после накопления обучающей выборки в течение 1 часа становится возможным определить отличия в процессах, функционирующих в системе, с вероятностью, близкой к 0,8.

На рис. 6 приведена вероятность правильной идентификации запущенной программы в зависимости от объема обучающей выборки для состояний, представленных на рис. 4, 5.

Предлагаемое решение не требует больших вычислительных затрат, подобная система может быть достаточно быстро обучена на различных методах машинного обучения и использоваться для обнаружения аномальных параметров функционирования автономного объекта в условиях, когда, осуществляя мероприятия по развертыванию системы в реальных условиях, на начальных этапах функционирования

можно произвести оценку статистических данных, на основе которых осуществить анализ, выявление и идентификацию аномалий функционирования. Статистика, полученная на основе проведенного эксперимента, показывает вид внешнего отклика анализируемой системы, достаточный для вероятностного определения состояния информационной безопасности.

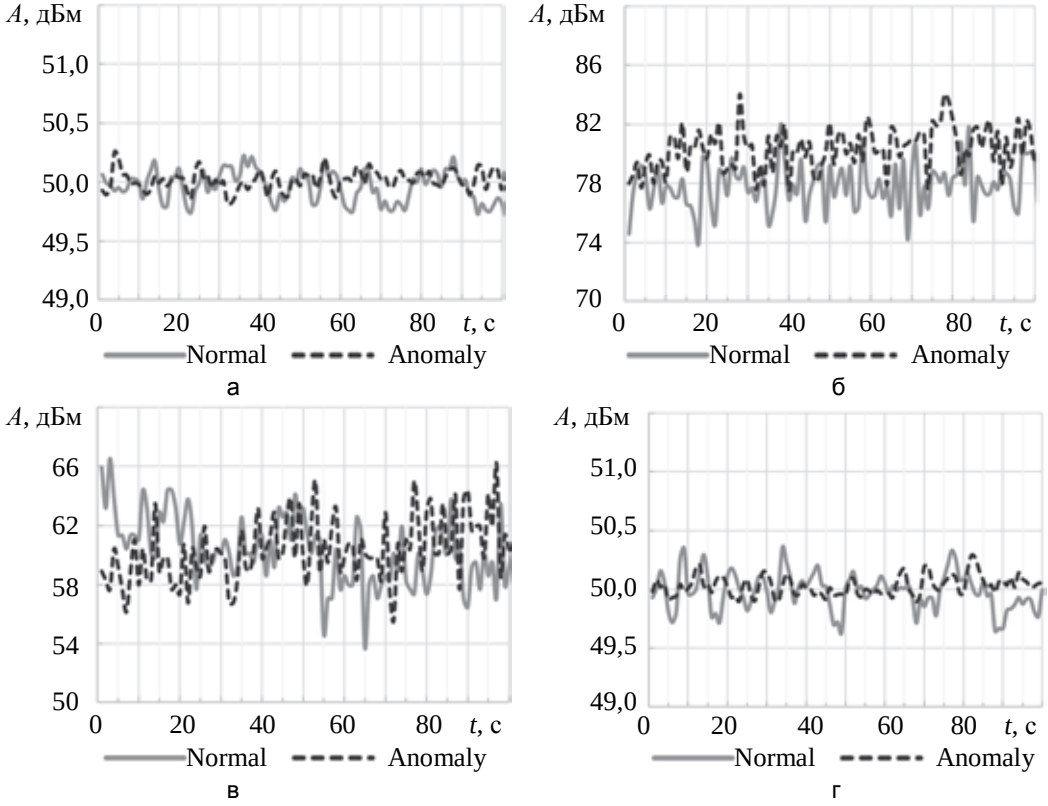


Рис. 5. Вид графиков колебаний амплитуды исследуемых пиков сигналов при нормальном функционировании системы и аномальном в случае изменения положения над поверхностью микросхемы для: датчиков типа АП Е3-50 (а); зондов ближнего поля типа NFP-3-P1 (б); зондов ближнего поля типа NFP-3-P2 (в); зондов ближнего поля типа NFP-3-P3 (г).
Normal – нормальное состояние, Anomaly – аномальное состояние

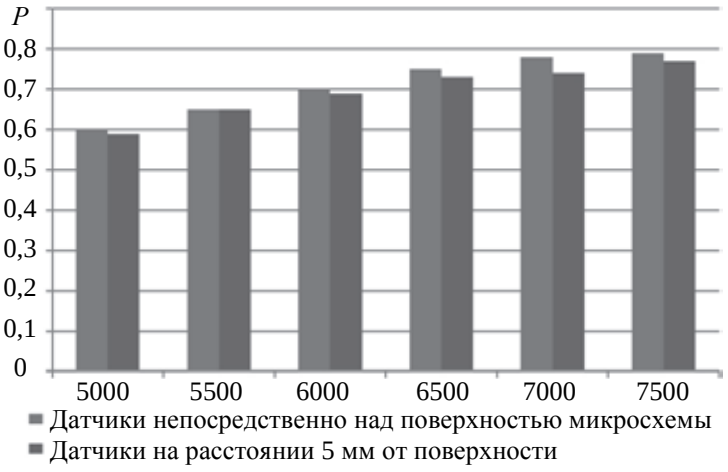


Рис. 6. Вероятность правильной идентификации запущенной программы (*P*) в зависимости от объема обучающей выборки (*n*) для состояний рис. 4, 5

Заключение

Типовым решением для выполнения таких требований по защите информации, как конфиденциальность и целостность информации, является применение специальных программно-аппаратных средств защиты информации, средств контроля защищенности информации и системы менеджмента информационной безопасности [12, 13]. Однако внедрение программных закладок и модификация кода мо-

гут происходить на таких этапах жизненного цикла, как разработка, производство, хранение, транспортировка, ввод в эксплуатацию, сопровождение и модернизация программных и технических средств, что повышает актуальность применения внешних независимых систем мониторинга информационной безопасности [14, 15]. Нарушитель может действовать на различных этапах жизненного цикла не только киберфизической системы, но и встроенных и интегрированных в нее средств защиты информации.

Предложенный метод мониторинга автономных объектов на основе статистических данных системы направлен на анализ внешних поведенческих признаков процессов, запущенных на вычислительном узле, не влияет на быстродействие и не затрагивает вычислительные и системные ресурсы узла.

Особенностью подхода является возможность быстрой адаптации и применения различного математического аппарата, методов машинного обучения для достижения заданного качества вероятностной оценки.

Реализации данного вида мониторинга не требует разработки сложных системных приложений, позволяет реализовывать различные архитектуры построения систем, производящие обработку на борту автономного объекта либо передачу данных и вычисление состояния на внешних вычислительных узлах систем мониторинга и контроля.

Литература

1. Котенко И.В., Саенко И.Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник РАН. 2014. Т. 84. № 11. С. 993–1001. doi: 10.7868/S0869587314110073
2. Rogachev G.N. Production method of describing automated controllers in the analysis of continuous-discrete control systems // Automatic Control and Computer Sciences. 2014. V. 48. N 5. P. 249–256. doi: 10.3103/S0146411614050095
3. Лещев С.В. Электронная культура и виртуальная реальность: третья цифровая волна НБИК-парадигмы // Вестник гуманитарного факультета ИГХТУ. 2014. Т. 7. С. 5–9.
4. Krivtsova I., Lebedev I., Sukhoparov M., Bazhayev N., Zikratov I., Ometov A., Andreev S., Masek P., Fujdiak R., Hosek J. Implementing a broadcast storm attack on a mission-critical wireless sensor network // Lecture Notes in Computer Science. 2016. V. 9674. P. 297–308. doi: 10.1007/978-3-319-33936-8_23
5. Сухопаров М.Е., Лебедев И.С. Метод выявления аномального поведения персональных сетей // Проблемы информационной безопасности. Компьютерные системы. 2017. № 1. С. 9–15.
6. Бажаев Н., Лебедев И.С., Кривцова И.Е. Анализ статистических данных мониторинга сетевой инфраструктуры для выявления аномального поведения локального сегмента системы // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 1. С. 92–99. doi: 10.17586/2226-1494-2017-92-99
7. Lebedev I.S., Bazhayev N., Sukhoparov M.E., Petrov V.I., Gurtov A.V. Analysis of the state of information security on the basis of surious emission electronic components // Proc. 20th Conference of Open Innovations Association FRUCT. St. Petersburg, Russia, 2017. P. 216–221. doi: 10.23919/FRUCT.2017.8071314
8. Nikolaevskiy I., Lukyanenko A., Polishchuk T., Polishchuk V.M., Gurtov A.V. isBF: scalable in-packet bloom filter based multicast // Computer Communications. 2015. V. 70. P. 79–85. doi: 10.1016/j.comcom.2015.05.002
9. Al-Naggar Y., Koucheryavy A. Fuzzy logic and Voronoi diagram using for cluster head selection in ubiquitous sensor networks // Lecture Notes in Computer Science. 2014. V. 8638. P. 319–330. doi: 10.1007/978-3-319-10353-2_28
10. Chehri A., Moutah H.T. Survivable and scalable wireless solution for e-health and emergency applications // Proc. 1st Int. Workshop on Engineering Interactive Computing Systems for Medicine and Health Care. Pisa, Italy, 2011. P. 25–29.
11. Сухопаров М.Е., Лебедев И.С. Анализ состояния информационной безопасности на основе побочного излучения электронных компонент // Проблемы информационной безопасности. Компьютерные системы. 2017. № 2. С. 92–98.
12. Royakkers L., van Est R. A literature review on new robotics: automation from love to war // International Journal of Social Robotics. 2015. V. 7. N 5. P. 549–570. doi: 10.1007/s12369-015-0295-x

References

1. Kotenko I.V., Saenko I.B. Creating new-generation cybersecurity monitoring and management systems. *Herald of the Russian Academy of Sciences*, 2014, vol. 84, no. 6, pp. 424–431. doi: 10.1134/S1019331614060033
2. Rogachev G.N. Production method of describing automated controllers in the analysis of continuous-discrete control systems. *Automatic Control and Computer Sciences*, 2014, vol. 48, no. 5, pp. 249–256. doi: 10.3103/S0146411614050095
3. Leshchev S.V. Electronic culture and virtual reality: the third digital wave of the NBIC paradigm. *Vestnik Gumanitarnogo Fakul'teta IGKhTU*, 2014, vol. 7, pp. 5–9. (In Russian)
4. Krivtsova I., Lebedev I., Sukhoparov M., Bazhayev N., Zikratov I., Ometov A., Andreev S., Masek P., Fujdiak R., Hosek J. Implementing a broadcast storm attack on a mission-critical wireless sensor network. *Lecture Notes in Computer Science*, 2016, vol. 9674, pp. 297–308. doi: 10.1007/978-3-319-33936-8_23
5. Sukhoparov M.E., Lebedev I.S. Detection method for personal networks anomalous behaviour. *Information Security Problems. Computer Systems*, 2017, no. 1, pp. 9–15. (In Russian)
6. Bazhayev N.A., Lebedev I.S., Krivtsova I.E. Analysis of statistical data from network infrastructure monitoring to detect abnormal behavior of system local segments. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 1, pp. 92–99. (In Russian) doi: 10.17586/2226-1494-2017-17-1-92-99
7. Lebedev I.S., Bazhayev N., Sukhoparov M.E., Petrov V.I., Gurtov A.V. Analysis of the state of information security on the basis of surious emission electronic components. *Proc. 20th Conference of Open Innovations Association FRUCT*. St. Petersburg, Russia, 2017, pp. 216–221. doi: 10.23919/FRUCT.2017.8071314
8. Nikolaevskiy I., Lukyanenko A., Polishchuk T., Polishchuk V.M., Gurtov A.V. isBF: scalable in-packet bloom filter based multicast. *Computer Communications*, 2015, vol. 70, pp. 79–85. doi: 10.1016/j.comcom.2015.05.002
9. Al-Naggar Y., Koucheryavy A. Fuzzy logic and Voronoi diagram using for cluster head selection in ubiquitous sensor networks. *Lecture Notes in Computer Science*, 2014, vol. 8638, pp. 319–330. doi: 10.1007/978-3-319-10353-2_28
10. Chehri A., Moutah H.T. Survivable and scalable wireless solution for e-health and emergency applications. *Proc. 1st Int. Workshop on Engineering Interactive Computing Systems for Medicine and Health Care*. Pisa, Italy, 2011, pp. 25–29.
11. Sukhoparov M.E., Lebedev I.S. Analysis of information security status based on adverse radiation of electronic components. *Information Security Problems. Computer Systems*, 2017, no. 2, pp. 92–98. (In Russian)
12. Royakkers L., van Est R. A literature review on new robotics: automation from love to war. *International Journal of Social Robotics*, 2015, vol. 7, no. 5, pp. 549–570. doi: 10.1007/s12369-015-0295-x
13. Chernyak L. Cyberphysical systems at start. *Open Systems.*

13. Черняк Л. Киберфизические системы на старте // Открытые системы. СУБД. 2014. № 2. С. 10–13.
14. Lee E.A., Neuendorffer S., Wirthlin M.J. Actor-oriented design of embedded hardware and software systems // Journal of Circuits, Systems and Computers. 2003. V. 12. N 3. P. 231–260. doi: 10.1142/S0218126603000751
15. Юсупов Р.М., Ронжин А.Л. От умных приборов к интеллектуальному пространству // Вестник РАН. 2010. Т. 80. № 1. С. 45–51.

Авторы

Семенов Виктор Викторович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-7216-769X, semenov@corp.ifmo

Лебедев Илья Сергеевич – доктор технических наук, доцент, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56321781100, ORCID ID: 0000-0001-6753-2181, lebedev@cit.ifmo.ru

Сухопаров Михаил Евгеньевич – кандидат технических наук, старший научный сотрудник, Санкт-Петербургский филиал АО «НПК «ТРИСТАН», Санкт-Петербург, 195220, Российская Федерация, Scopus ID: 57079293900, ORCID ID: 0000-0003-1798-8257, sukhoparovm@gmail.com

DBMS, 2014, no. 2, pp. 10–13. (In Russian)
14. Lee E.A., Neuendorffer S., Wirthlin M.J. Actor-oriented design of embedded hardware and software systems. *Journal of Circuits, Systems and Computers*, 2003, vol. 12, no. 3, pp. 231–260. doi: 10.1142/S0218126603000751
15. Yusupov R.M., Ronzhin A.L. From smart devices to smart space. *Herald of the Russian Academy of Sciences*, 2010, vol. 80, no. 1, pp. 63–68. (In Russian)

Authors

Victor V. Semenov – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-7216-769X,semenov@corp.ifmo.ru

Ilya S. Lebedev – D.Sc., Associate Professor, Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56321781100, ORCID ID: 0000-0001-6753-2181, lebedev@cit.ifmo.ru

Mikhail E. Sukhoparov – PhD, Senior scientific researcher, Saint Petersburg Branch AO «NPK «TRISTAN», Saint Petersburg, 195220, Russian Federation, Scopus ID: 57079293900, ORCID ID: 0000-0003-1798-8257, sukhoparovm@gmail.com