УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май—июнь 2019 Том 19 № 3 ISSN 2226-1494 http://ntv.itmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTCS
May—June 2019 Vol. 19 No 3 ISSN 2226-1494 http://ntv.itmo.ru/en/
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

УДК 004.021

doi: 10.17586/2226-1494-2019-19-3-492-498

ОБРАБОТКА СИГНАЛЬНОЙ ИНФОРМАЦИИ В ЗАДАЧАХ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОНОМНЫХ ОБЪЕКТОВ БЕСПИЛОТНЫХ СИСТЕМ

В.В. Семенов, И.С. Лебедев

Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), Санкт-Петербург, 199178, Российская Федерация
Адрес для переписки: semenov@corp.ifmo.ru

Информация о статье
Поступила в редакцию 15.03.19, принята к печати 19.04.19
Язык статьи — русский

Ссылка для цитирования: Семенов В.В., Лебедев И.С. Обработка сигнальной информации в задачах мониторинга информационной безопасности автономных объектов беспилотных систем // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 3. С. 492–498. doi: 10.17586/2226-1494-2019-19-3-492-498

Аннотация

Предмет исследования. Рассмотрены проблемные вопросы обеспечения информационной безопасности автономных беспилотных объектов. Раскрыты предпосылки, определяющие необходимость использования внешних систем мониторинга. Показан вид и статистические характеристики используемых для анализа и классификации звуковых сигналов. **Метод.** Предлагаемый подход анализа состояния информационной безопасности автономного объекта основан на методах классификации и позволяет идентифицировать текущее состояние на основе обработки оцифрованной акустической информации. Описан эксперимент, направленный на получение статистической информации о различных видах маневров беспилотного объекта при различном расположении аудиозаписывающего устройства. Полученные данные обрабатывались при помощи двухслойных нейронных сетей прямого распространения с сигмоидальной передаточной функцией в скрытых слоях. **Основные результаты.** Решена задача идентификации состояния информационной безопасности автономных беспилотных объектов на основе обработки акустической сигнальной информации, полученной по побочным каналам. Оцифрованная информация с акустического датчика (микрофона), расположенного статично в зоне проведения эксперимента, была классифицирована более точно, чем с микрофона, расположенного непосредственно на автономном объекте. При минимальном времени накопления статистической информации с использованием предложенного подхода становится возможным выявить различия в выполняемых беспилотным объектом маневрах, а следовательно, и состояние информационной безопасности объекта, с вероятностью, близкой к 0,7. **Практическая значимость.** Предложенный подход обработки сигнальной информации может быть использован в качестве дополнительного независимого элемента для определения состояния информационной безопасности автономных объектов беспилотных систем. Подход может быть быстро адаптирован с применением различного математического аппарата и методов машинного обучения для достижения заданного качества вероятностной оценки.

Ключевые слова
информационная безопасность, беспилотные автономные объекты, обработка данных, нейронные сети, системы мониторинга информационной безопасности

doi: 10.17586/2226-1494-2019-19-3-492-498

PROCESSING OF SIGNAL INFORMATION IN PROBLEMS OF MONITORING INFORMATION SECURITY OF UNMANNED AUTONOMOUS OBJECTS

V.V. Semenov, I.S. Lebedev

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Saint Petersburg, 199178, Russian Federation
Corresponding author: semenov@corp.ifmo.ru

Article info
Received 15.03.19, accepted 19.04.19
Article in Russian

For citation: Semenov V.V., Lebedev I.S. Processing of signal information in problems of monitoring information security of unmanned autonomous objects. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 3, pp. 492–498 (in Russian). doi: 10.17586/2226-1494-2019-19-3-492-498

Abstract
Subject of Research. We consider problematic issues of ensuring the information security of autonomous unmanned objects. Prerequisites are revealed that determine the need for external monitoring systems. The type and statistical characteristics are shown used for the analysis and classification of sound signals. **Method.** The proposed approach to analysis of information security state of an autonomous object is based on classification methods and allows identifying the current state based on the processing of digitized acoustic information. An experiment is described aimed at obtaining statistical information on various types of maneuvers of an unmanned object with a different location of the audio recorder. The obtained data were processed using two-layer feed-forward neural networks with sigmoid hidden neurons. **Main Results.** We have solved the problem of identifying the state of information security of autonomous unmanned objects based on processing of signal information obtained through side channels. Digitized information from acoustic sensor (microphone) located statically in the experiment area has been classified more accurately than from a microphone located directly on an autonomous object. With minimal accumulation of statistical information using the proposed approach, it has become possible to identify differences in maneuvers performed by unmanned objects, and, consequently, the state of information security of an object with a probability close to 0.7. **Practical Relevance.** The proposed approach for processing of signal information can be used as an additional independent element for information security state determination of autonomous objects of unmanned systems. The approach can be quickly adapted using various mathematical methods and machine learning to achieve probabilistic assessment with a given quality.

Keywords
information security, unmanned autonomous objects, data processing, neural networks, information security monitoring systems

Введение

Все более значимым направлением развития беспилотных систем является совершенствование теории и практики управления, контроля, использования мобильных удаленных автономных объектов, способных самостоятельно с применением средств искусственного интеллекта решать навигационные, транспортные, логистические задачи [1]. Такой подход предполагает децентрализованное управление, рассредоточение мобильных объектов, осуществление эпизодического взаимодействия, распределенного по пространственно-временной шкале, что вызывает необходимость осуществления ряда мер, направленных на обеспечение информационной безопасности (ИБ).

Анализ подходов к построению беспилотных систем обусловливает применение не только систем защиты, но и систем мониторинга состояния, оказывающихся основополагающими для решения задач идентификации внутренних и внешних процессов объекта. Классические подходы к защите информации, направленные на статистический анализ с целью предотвращения нарушения конфиденциальности, целостности, доступности циркулирующих данных, не позволяют гарантировать достижения заданной вероятности безопасного состояния автономного объекта и системы в целом.

Одним из дополнительных независимых элементов оценки состояния автономных агентов может быть информация, полученная через побочные каналы [2]. В рамках исследований на сегодняшний день выделено более десяти побочных каналов, на основе которых можно отслеживать состояния отдельных интеллектуальных агентов, среди которых акустический канал, электромагнитное излучение, временной канал и др. [3, 4].

Получаемые по ним данные возможно использовать не только для проведения различных атак [5, 6], но и для мониторинга и анализа состояния программно-аппаратной среды автономных агентов [7–9].

Большое число работ посвящено анализу информации, полученной по акустическому каналу [10]. В работе [11] исследователи используют для съема информации не только высокочувствительные микрофоны, но и микрофон обычного мобильного телефона. В настоящее время активно исследуются новые способы определения аномального состояния системы с помощью методов обработки сигналов на основе машинного обучения [12].

Внедрение беспилотных средств сопровождается необходимостью решения дополнительных проблемных вопросов обеспечения ИБ, таких как [13, 14]:

— 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 на предмет обнаружения не декларированных возможностей.

В связи с этим возникает необходимость разработки моделей, методов мониторинга ИБ, использующих дополнительные информационные источники, направленные на независимый анализ состояния мобильных удаленных автономных объектов транспортных систем.

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, методов мониторинга информационной безопасности автономных вычислительных средств [15, 16].

Реализация внешней контролирующей системы автономного беспилотного объекта может осуществляться на основе датчиков, которые в режиме реального времени регистрируют сигнал при выполнении разных действий объекта.

Идентификацию состояния автономного объекта возможно производить, используя данные внешних сигналов. Оцифрованный сигнал представляет из себя набор значений амплитуд A. Последовательность значений амплитуд $a_1, a_2,\ldots a_n$. будет определять последовательность показателей, получаемых в результате выполнения автономным объектом определенного действия.

Тогда необходимо в последовательности амплитуд сигнала $F = \{a_1, a_2,\ldots a_n\}$ обнаружить и идентифицировать сигнал $f = \{a_{1f}, a_{2f},\ldots a_{nf}\}$, который возникает при выполнении этого определенного действия.

Процесс распознавания происходит следующим образом. Из входного сигнала F выделяется образ f, а затем осуществляется сравнение амплитуд. На основе порогового коэффициента K делается вывод о нахождении требуемого сигнала в последовательности:

$$\frac{A_f}{A_F} \le K. \qquad (1)$$

Решение задачи (1) сводится к задаче классификации, где множество классов принимает значения $Y = \{Y_0, Y_1\}$, Y_0 — безопасное состояние, где совершается идентифицируемое действие, вызванное управляющей командой и Y_1 — небезопасное состояние, при котором идентифицируемое действие в данный момент отличается от вызванного управляющей командой.

Предлагаемый подход

Удаленные автономные объекты представляют из себя сложные системы, в которых одновременно протекает огромное множество процессов. Каждый процесс характеризуется внешними сигналами, которые можно получить по побочным каналам в результате функционирования электронных или механических компонент, выполнения объектом каких-либо команд и действий.

В качестве подходов, обеспечивающих дополнительный контроль состояния, можно использовать анализ поведенческих характеристик объекта. Изменение параметров электромагнитных излучений, акустических шумов, появление различных вибраций при выполнении действий и маневров может давать дополнительную информацию о состоянии. Анализ отклонений, выявляемых по таким данным, предоставляет дополнительную информацию для принятия решения, что является определенным преимуществом в условиях неопределенности.

Для идентификации процесса таким способом необходима обучающая выборка. Поэтому на первом шаге выполняется накопление данных при выполнении заранее заданных маневров беспилотным средством (рис. 1). Второй шаг заключается в обработке полученной информации, где происходит удаление шумов. Третий шаг связан с формированием обучающей выборки, на основе которой будет проводиться анализ.

На основе информации о внешних управляющих воздействиях система обладает данными о разрешенном маневре беспилотного средства в заданный момент времени. Анализируя информацию обучающей выборки и текущих значений делается вывод о проводимом беспилотным средством маневре. Таким образом, в случае отличия выявленного маневра от разрешенного, управляющая система делает вывод о нахождении управляемой системы в небезопасном (аномальном) состоянии Y_1.

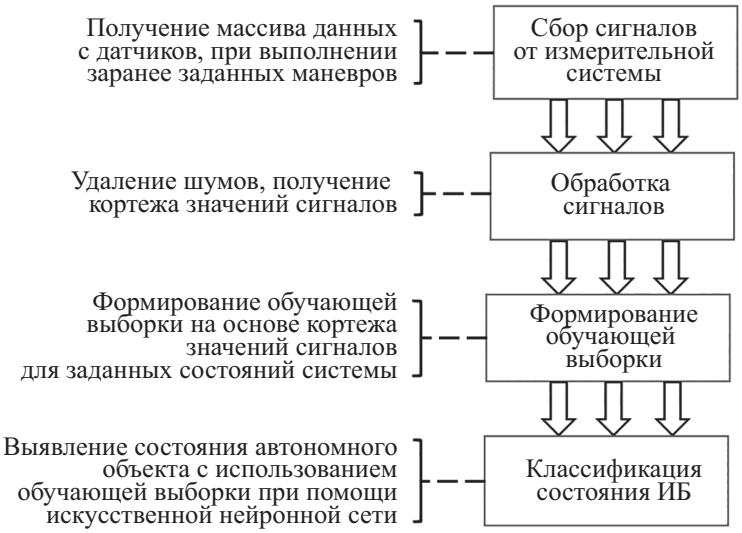

Рис. 1. Предлагаемый подход

Формирование обучающей выборки, где на каждое действие или выполняемую команду накапливается информация снимаемых данных сигналов, позволяет применить различные методы машинного обучения.

Эксперимент

В автономных беспилотных элементах системы в зависимости от внешних факторов для выполнения функциональных возможностей, связанных, например, с маневром по скорости или по направлению, возникают ситуации, когда необходимо определить текущее состояние объекта. Оценка состояния объекта может быть произведена на основе сравнения с эталонной выборкой [17, 18].

Для анализа возможностей приведенного подхода был проведен эксперимент, направленный на получение поведенческих характеристик различных маневров беспилотного транспортного средства. В качестве независимого внешнего канала выбран акустический.

Испытуемое беспилотное средство совершало заданные с пульта управления маневры, такие как движение вперед прямо (↑), назад прямо (↓), вперед направо (↗), вперед налево (↖), назад направо (↘), назад налево (↙). Для получения обучающей выборки при помощи датчика, представляющего из себя микрофон (МК), производилась многоразовая запись параметров каждого маневра. В случае 1 (рис. 2, *а*) акустический датчик (микрофон) располагался непосредственно на корпусе испытуемого беспилотного транспортного средства, в случае 2 (рис. 2, *б*) — был статично установлен справа от зоны проведения эксперимента, как схематично показано на рис. 2.

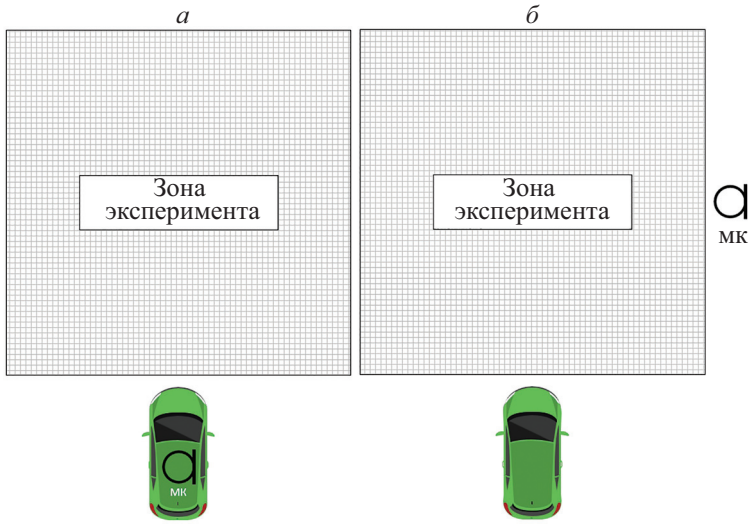

Рис. 2. Схема расположения аудиозаписывающего устройства во время проведения эксперимента: микрофон закреплен на корпусе беспилотного транспортного средства (*а*), микрофон справа от зоны проведения эксперимента (*б*)

Полученные данные были оцифрованы. Продолжительность разных маневров отличалась и составляла от 2,5 до 3,5 с. На рис. 3 приведен внешний вид сигналов для различных маневров для случая 1 (рис. 3, *а*) — акустический датчик расположен на беспилотном транспортном средстве и для случая 2 (рис. 3, *б*) — статично установлен справа от зоны проведения эксперимента. Сигналы справа характеризуются большей монотонностью и амплитудой.

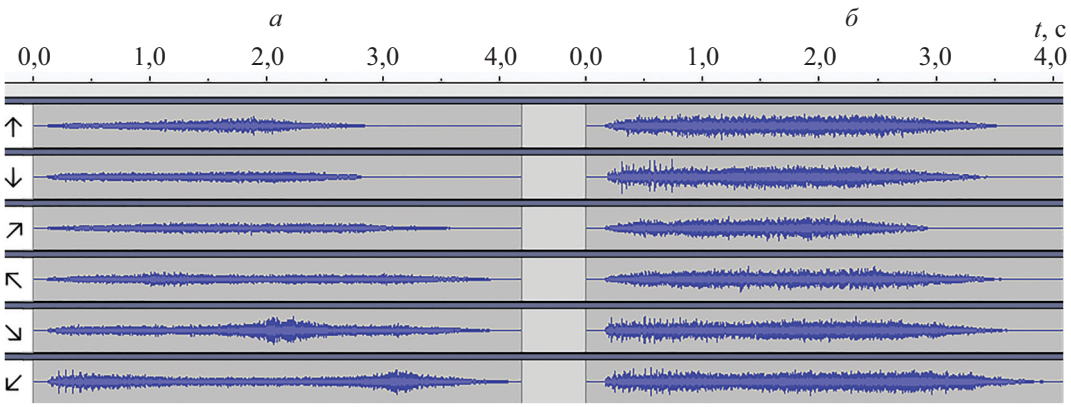

Рис. 3. Внешний вид сигналов. Акустический датчик расположен на беспилотном транспортном средстве (*а*) и микрофон статично установлен справа от зоны проведения эксперимента (*б*)

Из каждого непрерывного по времени сигнала при его дискретизации было равномерно взято 5000 отсчетов. Полученные значения были обработаны при помощи двухслойных нейронных сетей прямого распространения с сигмоидальной передаточной функцией в скрытых слоях (рис. 4). Использовалось программное обеспечение (ПО) MATLAB R2018b Update 2, приложение Neural Network Pattern Recognition пакета DeepLearning Toolbox. Число входных нейронов — 1, оно определяется единственным измеряемым параметром — амплитудой сигнала, количество скрытых нейронов — 300. Количество выходных нейронов, т. е. число элементов в целевом векторе равно количеству исследуемых состояний автономного объекта — 6. Выходы нейронной сети представляют собой значения вероятностей, с которыми исследуемое состояние относится к определенному классу. Производилась классификация по шести состояниям.

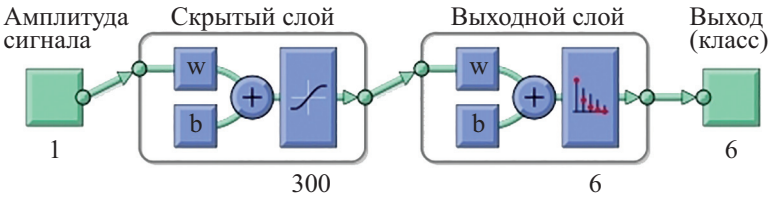

Рис. 4. Схема используемой двухслойной нейронной сети прямого распространения (ПО MATLAB R2018b). **w** — матрицы весов, **b** — векторы смещений

Для формирования обучающей выборки использовалось 70 % значений, 15 % значений использовалось в качестве тестового и еще 15 % — в качестве проверочного набора. В табл. 1 и 2 приведены результаты классификации по шести классам, соответствующим каждому маневру для различных вариантов расположения записывающего устройства.

Таблица 1. Результаты классификации нейронной сетью по шести классам для случая 1 — микрофон расположен на беспилотном транспортном средстве

Маневры		Истинный класс						Всего	Точность
		↑	↓	↗	↖	↘	↙		
Расчетный класс	↑		2639	0	0	0	0	16247	0,8376
	↓	1392			0	1528	0	15095	0,6590
	↗	0	1398		2833	4185	1942	19007	0,4550
	↖	0	0	1201		0	1036	13598	0,8355
	↘	0	1015	2598	0		3212	15279	0,5533
	↙	0	0	325	806	833		10774	0,8177
Всего		15000	15000	15000	15000	15000	15000		
Точность		0,9072	0,6632	0,5766	0,7574	0,5636	0,5873		

Общая точность выбранного классификатора (overall accuracy) для случая 1: 60830/90000 = 0,6759.

Таблица 2. Результаты классификации нейронной сетью по шести классам для случая 2 — микрофон статично установлен справа от зоны проведения эксперимента

Маневры		Истинный класс						Всего	Точность
		↑	↓	↗	↖	↘	↙		
Расчетный класс	↑		1074	405	381	603	375	15207	0,8134
	↓	753		594	360	759	576	14310	0,7874
	↗	405	765		1491	912	1035	15141	0,6957
	↖	738	1068	1326		1461	1746	16503	0,6159
	↘	267	543	1233	1569		1563	14430	0,6414
	↙	468	282	909	1035	2010		14409	0,6735
Всего		15000	15000	15000	15000	15000	15000		
Точность		0,8246	0,7512	0,7022	0,6776	0,6170	0,6470		

Общая точность выбранного классификатора (overall accuracy) для случая 2: 63294/90000 = 0,7033.

Как видно из табл. 2, система мониторинга позволяет выявить различия в параметрах маневров с вероятностью близкой к 0,7.

Произведена оценка соотношения корректных (*T*) результатов классификации для каждого случая (рис. 5).

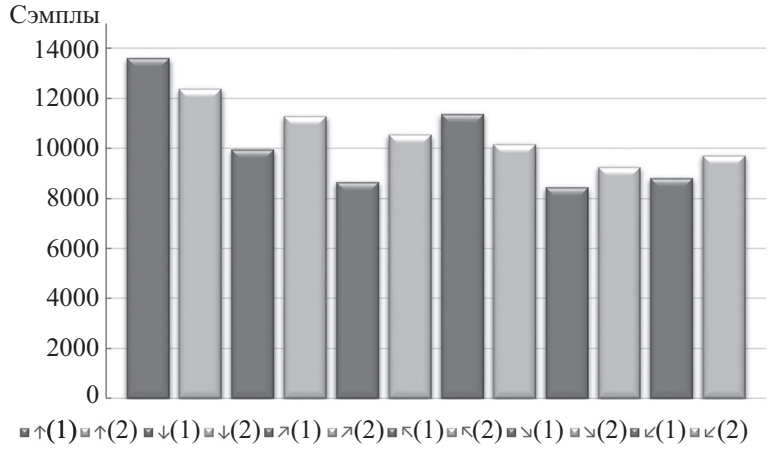

Рис. 5. Соотношение корректных результатов классификации для случаев:
1 — микрофон расположен на беспилотном транспортном средстве;
2 — микрофон статично установлен справа от зоны проведения эксперимента

Заключение

Одним из подходов определения состояния информационной безопасности может быть использование внешнего, например, акустического канала.

Применение предлагаемого подхода для анализа состояния мобильных объектов беспилотных систем направлено на преодоление следующих процессов:

— текущее состояние вычислительного процесса закрыто от наблюдателя;

— вычислительный процесс протекает в мультизадачном режиме, выполняя псевдопараллельно решение отдельных задач функционирования системы;

— значения физических параметров, измеряемых в разные моменты функционирования, имеют корреляцию с потреблением энергии, временем вычислений, электромагнитным излучением и т. п.

Предложенный подход дает возможность осуществления контроля состояния объекта на основе внешнего независимого канала.

Точность определения состояния информационной безопасности напрямую зависит от точности классификации обрабатываемых системой данных, а проведенный эксперимент показал, что даже с учетом зашумленности при помощи аудиозаписи маневра становится возможным выявить различия с вероятностью близкой к 0,7.

Литература

1. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities // Proc. 1st Int. Workshop on Safety and Security in Multi-Agent Systems (SASEMAS). 2004. P. 85–101.
2. Семенов В.В., Лебедев И.С., Сухопаров М.Е. Идентификация состояния отдельных элементов киберфизических систем на основе внешних поведенческих характеристик // Прикладная информатика. 2018. Т. 13. № 5(77). С. 72–83.
3. Hayashi Y.I., Homma N., Watanabe T., Price W.O., Radasky W.A. Introduction to the special section on electromagnetic information security // Proc. IEEE Transactions on Electromagnetic Compatibility. 2013. V. 55. N 3. P. 539–546. doi: 10.1109/temc.2013.2255294
4. Kocher P., Jaffe J., Jun B. Introduction to differential power analysis and related attacks // Lecture Notes in Computer Science. 1998. V. 1109. P. 104–113.
5. de Souza Faria G., Kim H.Y. Differential audio analysis: a new side-channel attack on PIN pads // International Journal of Information Security. 2019. V. 18. N 1. P. 73–84. doi: 10.1007/s10207-018-0403-7
6. Gupta H., Sural S., Atluri V., Vaidya J. A side-channel attack on smartphones: Deciphering key taps using built-in microphones // Journal of Computer Security. 2018. V. 26. N 2. P. 255–281. doi: 10.3233/JCS-17975

References

1. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities. *Proc. 1st Int. Workshop on Safety and Security in Multi-Agent Systems*, SASEMAS, 2004, pp. 85–101.
2. Semenov V.V., Lebedev I.S., Sukhoparov M.E. Identification of the state of individual elements of cyber-physical systems based on external behavioral characteristics. *Journal of Applied Informatics*, 2018, vol. 13, no. 5, pp. 72–83 (in Russian).
3. Hayashi Y.I., Homma N., Watanabe T., Price W.O., Radasky W.A. Introduction to the special section on electromagnetic information security. *Proc. IEEE Transactions on Electromagnetic Compatibility*, 2013, vol. 55, no. 3, pp. 539–546. doi: 10.1109/temc.2013.2255294
4. Kocher P., Jaffe J., Jun B. Introduction to differential power analysis and related attacks. *Lecture Notes in Computer Science*, 1998, vol. 1109, pp. 104–113.
5. de Souza Faria G., Kim H.Y. Differential audio analysis: a new side-channel attack on PIN pads. *International Journal of Information Security*, 2019, vol. 18, no. 1, pp. 73–84. doi: 10.1007/s10207-018-0403-7
6. Gupta H., Sural S., Atluri V., Vaidya J. A side-channel attack on smartphones: Deciphering key taps using built-in microphones. *Journal of Computer Security*, 2018, vol. 26, no. 2, pp. 255–281. doi: 10.3233/JCS-17975

7. Сухопаров М.Е., Семенов В.В., Лебедев И.С. Мониторинг информационной безопасности элементов киберфизических систем с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 59–60.
8. 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
9. Semenov V.V., Sukhoparov M.E., Lebedev I.S. An approach to classification of the information security state of elements of cyber-physical systems using side electromagnetic radiation // Lecture Notes in Computer Science. 2018. V. 11118. P. 289–298. doi: 10.1007/978-3-030-01168-0_27
10. Al Faruque M.A., Chhetri S.R., Canedo A., Wan J. Acoustic side-channel attacks on additive manufacturing systems // Proc. ACM/IEEE 7th Int. Conf. on Cyber-Physical Systems. Vienna, Austria, 2016. doi: 10.1109/ICCPS.2016.7479068
11. Genkin D., Shamir A., Tromer E. Acoustic cryptanalysis // Journal of Cryptology. 2017. V. 30. N 2. P. 392–443. doi: 10.1007/s00145-015-9224-2
12. Farrokhmanesh M., Hamzeh A. Music classification as a new approach for malware detection // Journal of Computer Virology and Hacking Techniques. 2018. P. 1–20. doi: 10.1007/s11416-018-0321-2
13. Lebedev I., Krivtsova I., Korzhuk V., Bazhayev N., Sukhoparov M., Pecherkin S., Salakhutdinova K. The analysis of abnormal behavior of the system local segment on the basis of statistical data obtained from the network infrastructure monitoring // Lecture Notes in Computer Science. 2016. V. 9870. P. 503–511. doi: 10.1007/978-3-319-46301-8_42
14. Мариненков Е.Д., Викснин И.И., Жукова Ю.А., Усова М.А. Анализ защищенности информационного взаимодействия группы беспилотных летательных аппаратов // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 5. С. 817–825. doi: 10.17586/2226-1494-2018-18-5-817-825
15. Семенов В.В., Лебедев И.С. Анализ состояния информационной безопасности объектов транспортных систем // XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». СПб., 2018. С. 324–325.
16. Sridhar P., Sheikh-Bahaei S., Xia S., Jamshidi M. Multi agent simulation using discrete event and soft-computing methodologies // Proc. IEEE Int. Conf. on Systems, Man and Cybernetics. 2003. V. 2. P. 1711–1716. doi: 10.1109/icsmc.2003.1244659
17. 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
18. Кривцова И.Е., Салахутдинова К.И., Кузьмич П.А. Метод построения сигнатур исполняемых файлов с целью их идентификации // Вестник полиции. 2015. Т. 5. № 3(5). С. 97–105. doi: 10.13187/vesp.2015.5.97

7. Sukhoparov M.E., Semenov V.V., Lebedev I.S. Information security monitoring of elements of cyber-physical systems using artificial neural networks. *Metody i Tekhnicheskie Sredstva Obespecheniya Bezopasnosti Informatsii*, 2018, no. 27, pp. 59–60 (in Russian).
8. 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
9. Semenov V.V., Sukhoparov M.E., Lebedev I.S. An approach to classification of the information security state of elements of cyber-physical systems using side electromagnetic radiation. *Lecture Notes in Computer Science*, 2018, vol. 11118, pp. 289–298. doi: 10.1007/978-3-030-01168-0_27
10. Al Faruque M.A., Chhetri S.R., Canedo A., Wan J. Acoustic side-channel attacks on additive manufacturing systems. Proc. ACM/*IEEE 7th Int. Conf. on Cyber-Physical Systems*. Vienna, Austria, 2016. doi: 10.1109/ICCPS.2016.7479068
11. Genkin D., Shamir A., Tromer E. Acoustic cryptanalysis. *Journal of Cryptology*, 2017, vol. 30, no. 2, pp. 392–443. doi: 10.1007/s00145-015-9224-2
12. Farrokhmanesh M., Hamzeh A. Music classification as a new approach for malware detection. *Journal of Computer Virology and Hacking Techniques*, 2018, pp. 1–20. doi: 10.1007/s11416-018-0321-2
13. Lebedev I., Krivtsova I., Korzhuk V., Bazhayev N., Sukhoparov M., Pecherkin S., Salakhutdinova K. The analysis of abnormal behavior of the system local segment on the basis of statistical data obtained from the network infrastructure monitoring. *Lecture Notes in Computer Science*, 2016, vol. 9870, pp. 503–511. doi: 10.1007/978-3-319-46301-8_42
14. Marinenkov E.D., Viksnin I.I., Zhukova Iu.A., Usova M.A. Analysis of information interaction security within group of unmanned aerial vehicles. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 5, pp. 817–825 (in Russian). doi: 10.17586/2226-1494-2018-18-5-817-825
15. Semenov V.V., Lebedev I.S. Analysis of information security of transport systems. *Proc. 16th Int. Conf. on Regional Informatics RI-2018*. St. Petersburg, 2018, pp. 324–325 (in Russian).
16. Sridhar P., Sheikh-Bahaei S., Xia S., Jamshidi M. Multi agent simulation using discrete event and soft-computing methodologies. *Proc. IEEE Int. Conf. on Systems, Man and Cybernetics*, 2003, vol. 2, pp. 1711–1716. doi: 10.1109/icsmc.2003.1244659
17. 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
18. Krivtsova I.E., Salakhutdinova K.I., Kuz'mich P.A Method of construction the signatures of executable files for identification purposes. *Vestnik Policii*, vol. 5, no. 3, pp. 97–105 (in Russian). doi: 10.13187/vesp.2015.5.97

Авторы

Семенов Виктор Викторович — младший научный сотрудник, Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), Санкт-Петербург, 199178, Российская Федерация, Scopus ID: 57204123255, ORCID ID: 0000-0002-7216-769X, semenov@corp.ifmo.ru

Лебедев Илья Сергеевич — доктор технических наук, профессор, заведующий лабораторией, Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), Санкт-Петербург, 199178, Российская Федерация, Scopus ID: 56321781100, ORCID ID: 0000-0001-6753-2181, lebedev@cit.ifmo.ru

Authors

Viktor V. Semenov — Junior scientific researcher, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Saint Petersburg, 199178, Russian Federation, Scopus ID: 57204123255, ORCID ID: 0000-0002-7216-769X, semenov@corp.ifmo.ru

Ilya S. Lebedev — D.Sc., Professor, Laboratory head, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Saint Petersburg, 199178, Russian Federation, Scopus ID: 56321781100, ORCID ID: 0000-0001-6753-2181, lebedev@cit.ifmo.ru