УДК 004.021 DOI: 10.17587/it.26.424-430

В. В. Семенов, мл. науч. сотр., e-mail: v.semenov@iias.spb.su,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Мониторинг информационной безопасности беспилотных транспортных средств с использованием цифрового акселерометра

Рассматривается задача определения состояния информационной безопасности беспилотного транспортного средства внешней системой мониторинга. Эффективность решения задачи оценивается общей точностью классификации состояний объекта. Предлагается метод, основанный на анализе и классификации спектральных данных, регистрируемых с помощью цифрового трехосевого акселерометра, установленного на борту транспортного средства. Проведен эксперимент, направленный на исследование предложенного метода. В результате эксперимента показана принципиальная возможность использования данного побочного канала информации для использования в системах мониторинга информационной безопасности. Общая точность выбранного классификатора на основе алгоритма k-NN составила 0,82.

Ключевые слова: *информационная безопасность, беспилотные транспортные средства, системы мониторинга информационной безопасности, побочные каналы, акселерометр, обработка многомерных данных*

Введение

Современное развитие систем управления транспортом характеризуется внедрением и все более частым применением беспилотных транспортных средств (летающих объектов, автомобилей, поездов) для решения широкого круга задач [1]. Одним из направлений исследований и развития этой области является совершенствование теории и практики управления, контроля и использования беспилотных транспортных средств (БТС), способных самостоятельно с применением средств искусственного интеллекта решать отдельные задачи.

Подобный подход предусматривает децентрализованное управление транспортным средством, которое может осуществляться как с пульта управления, так и по заранее заданному алгоритму — автономно, что вызывает необходимость осуществления ряда мер, направленных на обеспечение информационной безопасности. Такие решения должны быть защищены от преднамеренных и непреднамеренных деструктивных воздействий, что вызывает необходимость внедрения не только систем защиты, но и систем мониторинга состояния. Классические подходы к защите информации, выражающиеся в противодействии несанкционированному доступу к данным, полностью не гарантируют достижения безопасного состояния.

В связи с вышесказанным возникает необходимость разработки моделей и методов мониторинга информационной безопасности (ИБ), использующих дополнительные источники, обеспечивающие независимый анализ состояния удаленных БТС.

1. Постановка задачи

Эффективность решений в области ИБ устройств, находящихся вне контролируемой зоны, связана с развитием научно-методического аппарата, предназначенного для повышения качественных показателей идентификации состояния защищенности. Защита киберфизических систем управления транспортом от атак является важной, но сложной задачей [2, 3]. Для ее решения необходима разработка моделей и методов мониторинга информационной безопасности автономных вычислительных средств [4, 5], учитывающих особенности киберфизических систем [6].

Одним из источников, позволяющих осуществлять анализ состояния ИБ, являются побочные каналы. В работе [7] приведен обзор некоторых методов определения аномального функционирования устройств с использованием информации побочных каналов. Выбор побочного канала зависит от конкретных при-

кладных задач и типа внешней системы мониторинга [8]. Широко применяются на практике побочные электромагнитные излучения и наводки [9, 10], видимое излучение, акустический канал [11] и др.

В работах [12, 13] применительно к системам защиты и мониторинга ИБ рассматривались решения, позволяющие проводить в основном бинарную классификацию, определяющую опасные и безопасные состояния. Однако в ряде случаев для оперативного реагирования на инцидент важно знать не только факт деструктивного воздействия, но и время начала вмешательства [14], а также подробности поведения контролируемого объекта. В случае с БТС это должны быть как конкретные координаты, так и значения параметров ускорения во время выполнения поставленных задач.

Таким образом, поставлена задача разработки метода мониторинга ИБ БТС, позволяющего осуществлять внешний независимый анализ состояния и отличающегося от известных, использующих классификацию, применением специализированного признакового пространства, которое базируется на совокупности оцифрованных последовательностей проекций ускорения и спектральных характеристиках.

Описать состояние исследуемого объекта можно с использованием в качестве источника полезной информации внешних каналов [15]. Предлагается модель профиля, описывающая состояние БТС на основе данных акселерометра с помощью последовательности проекций ускорения после дискретизации сигнала по времени:

$$\psi(t) = \begin{vmatrix} a_x(0) & a_x(1) & \dots & a_x(m) \\ a_y(0) & a_y(1) & \dots & a_y(m) \\ a_z(0) & a_z(1) & \dots & a_z(m) \end{vmatrix}, \qquad (1)$$

где $a_x(t)$, $a_y(t)$, $a_z(t)$ — проекции ускорения на соответствующую ось в момент времени t.

В случае использования спектрального преобразования кортеж (1) приобретает вид:

$$\Psi(f) = \begin{vmatrix} I_x(0) & I_x(1) & \dots & I_x(m) \\ I_y(0) & I_y(1) & \dots & I_y(m) \\ I_z(0) & I_z(1) & \dots & I_z(m) \end{vmatrix}, \qquad (2)$$

где $I(f)$ — значение спектральной интенсивности на частоте f.

Мониторинг состояния информационной безопасности становится возможным после применения различных классификаторов и методов машинного обучения к информации (2), полученной с датчиков. Отклонение от нормального состояния отражается во внезапном изменении трасс сигналов. Измененный вход спектра приведет к тому, что соответствующий ему вектор скрытого состояния отойдет от ожидаемого вектора в пространстве состояний.

2. Предлагаемый метод

Предлагаемый метод основан на модели профиля исследуемых объектов и позволяет определить отклонения от безопасного функционирования БТС в целях дальнейшего реагирования на выявленные инциденты. Стоит отметить, что применяя данный метод, нельзя однозначно судить о типе воздействия и о его преднамеренном или непреднамеренном характере. Нахождение устройства под атакой или иное непреднамеренное воздействие вызывает различные аномалии во внутренних вычислительных процессах объекта, что влечет за собой изменение потребляемой мощности, параметров побочного излучения, увеличение времени задержек и т.д. Целью злоумышленника может являться получение как полного, так и частичного (эпизодического) контроля над атакуемым устройством. Такая атака может, в частности, проявляться при использовании злоумышленником атакующего устройства, способного выдавать свои управляющие команды за команды легального пользователя, или (в случае автономной эксплуатации) при внесении злоумышленником деструктивных изменений в рабочую программу движения БТС. На рис. 1 схематично представлен предлагаемый метод.

Первой стадией является обучение, в результате которого выявляются текущие параметры

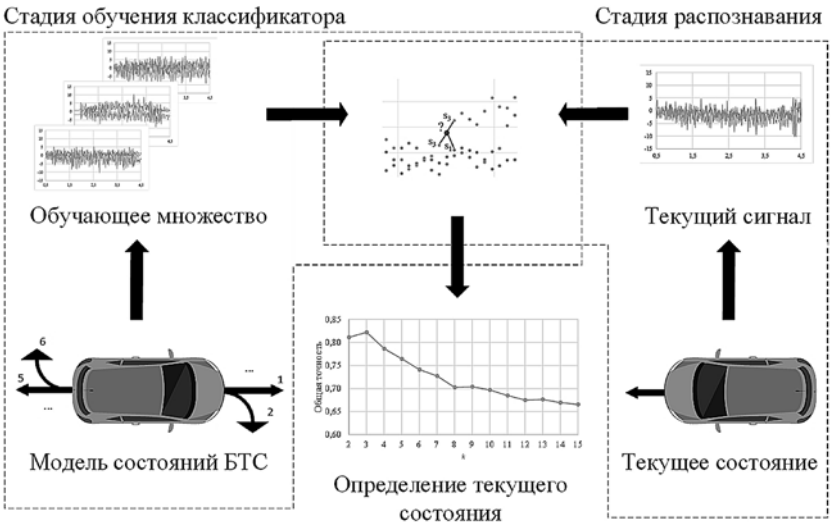

Рис. 1. Метод мониторинга состояний БТС

ускорения, описывающие состояние объекта. Обучение проводится на заранее определенных последовательностях, отражающих поведение объекта в известных состояниях. Накопленные статистические данные в дальнейшем позволяют определить критерии, на основе которых возможно реализовывать классификаторы для обнаружения аномалий.

В результате деструктивного воздействия происходят изменения выполнения управляющих последовательностей. Классифицируя спектры проекций ускорения различных состояний, можно идентифицировать аномальные состояния.

Для классификации был использован алгоритм k-NN (k ближайших соседей), реализованный в среде MATLAB R2019b. Достоинствами метода классификации состояний с использованием алгоритма k-NN являются простота и отсутствие фазы обучения, классификация проводится непосредственно в процессе применения модели над обучающим множеством и исследуемым процессом. Алгоритм [16] классифицирует все доступные точки спектра по показателям их сходства. В качестве метрики для определения сходства между двумя точками спектра можно использовать евклидово расстояние:

$$d(p,q) = \sqrt{\sum_{k=1}^{n} (p_k - q_k)^2}. \qquad (3)$$

Для каждой точки спектральных данных вычисляются расстояния (3) до других доступных точек, выбираются ближайшие k соседей и для каждого класса вычисляются условные вероятности. Точка данных будет принадлежать классу с наибольшей условной вероятностью. k является гиперпараметром модели и должен быть установлен до проведения классификации. Путем варьирования данного гиперпараметра можно определить его оптимальное значение для исследуемого набора данных. На этапе оптимизации используемого алгоритма при фиксированном k с использованием обучающей выборки евклидово расстояние показало наибольшие значения точности.

3. Эксперимент

Анализ возможностей мониторинга состояния объекта проводился на основе данных эксперимента, в котором БТС подвергалось внешнему воздействию при выполнении различных маневров. Предварительный этап эксперимента состоял в обучении внешней контролирующей системы на основе характеристик сигналов, снимаемых с помощью акселерометра, установленного на борту БТС, при выполнении маневров. Каждый маневр повторялся пять раз для накопления достоверной статистической информации. Схема эксперимента представлена на рис. 2.

Измерения линейного ускорения БТС выполнены с помощью цифрового трехосевого акселерометра BMC150 Acceleration Sensor фирмы Bosch Sensortec GmbH (Германия). Интервал между двумя последовательными измерениями 0,0096 с. Максимальное измеряемое прибором линейное ускорение 19,6133 м/с^2 (в пересчете на проекцию по любой из осей). Данные, полученные от измерительного устройства, регистрировались внешней контролирующей системой.

Определение пространственной ориентации БТС выполнялось относительно вектора гравитационного поля Земли **g**. Углы наклона измерялись, как показано на рис. 3.

Исходя из этого, величины проекций векторов ускорения a_x, a_y, a_z по осям x, y, z можно рассчитать по формулам

$$a_x = g\sin\theta\cos\varphi; \qquad (4)$$

$$a_y = -g\sin\theta\sin\varphi; \qquad (5)$$

$$a_z = g\cos\theta, \qquad (6)$$

где g — модуль измеренного акселерометром ускорения.

Используемая конечная система координат показана на рис. 4. Начало координат нахо-

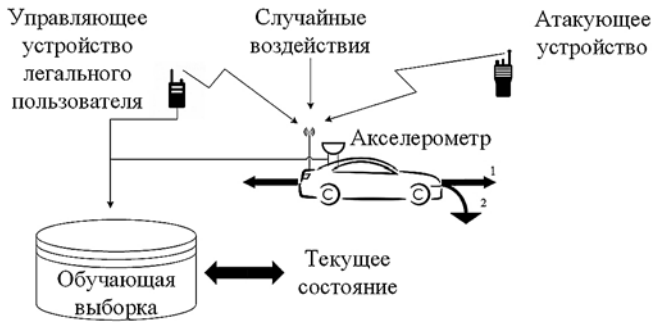

Рис. 2. Схема эксперимента

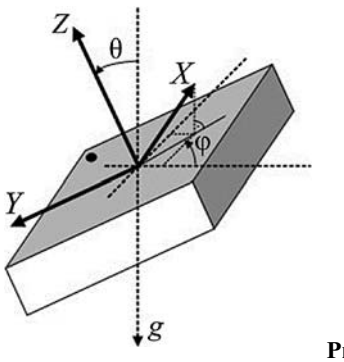

Рис. 3. Определение пространственной ориентации

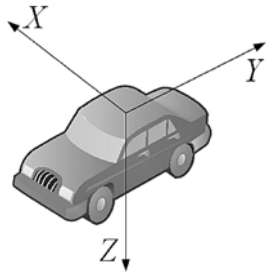

Рис. 4. Используемая конечная система координат относительно БТС

дится в верхней центральной точке БТС. Если БТС движется вперед, то ось Y будет направлена назад прямо, ось X — перпендикулярно вправо по направлению движения, а ось Z — вертикально вниз.

Проведен эксперимент, направленный на получение статистических портретов различных маневров объекта на основе данных статично установленного на борту цифрового акселерометра, фиксирующего ускорение БТС. По формулам (4)—(6) ускорение пересчитано в проекции по осям. Измеренные значения могут передаваться по беспроводной сети или обрабатываться непосредственно на самом контролирующем измерительном устройстве.

В ходе эксперимента испытуемое БТС совершало заданные с пульта управления маневры, относимые к безопасным (классы 1—3) — движение "вперед прямо", "вперед направо", "вперед налево" и к небезопасным (классы 4—6), когда в процессы функционирования моделировалось вмешательство злоумышленника — "движение прямо" с перехватом сигнала и периодическим внесением с пульта злоумышленника команд "направо", "налево", "назад". Каждый маневр повторялся шесть раз, данные фиксировались внешней системой. Показания акселерометра в состоянии останова транспортного средства также фиксировались, но не участвовали в общей классификации, поскольку данное состояние значительно отличается от других (рис. 5) определяется с точностью 0,99.

В состоянии останова наличие смещения значений проекций линейного ускорения по осям X и Y относительно нуля свидетельствует о расположении датчика под углом. Поскольку модель определяет отклонения от нормального состояния, обнаружение аномального функционирования возможно при любом начальном расположении датчика, главным условием является лишь его статичное расположение в период накопления обучающей выборки и классификации состояния ИБ. В случае смены пространственного расположения датчика исходя из архитектуры конкретного (одного и того же) устройства возможен перенос зависимостей.

На рис. 6 представлен график проекций ускорения по трем осям для случая движение "вперед прямо".

Поскольку ось Z направлена вертикально вверх, а эксперимент проводился на ровной поверхности (без изменения уровня высоты), то на проекцию a_z ускорения на ось Z самое большое влияние всегда будет оказывать величина ускорения свободного падения g. В дальнейшем, с учетом указанных ограничений эксперимента, будем считать, что a_z для исследуемого БТС не несет полезной информации и для наглядности уберем a_z из последующих графиков.

На рис. 7 представлен график проекций ускорения по двум осям для случая движение "вперед направо". По сравнению с графиком для случая 1 (см. рис. 6) наблюдается четко выраженное увеличение проекции ускорения на ось X (ось направлена вправо по направлению движения).

В случае движения "вперед налево" наблюдается закономерное снижение проекции ускорения на ось X. Для других случаев (состояния 3—6) также явно прослеживается прямая зависимость величин проекций ускорения по осям от совершаемых маневров.

Недостатком применения зависимостей линейного ускорения от времени для целей проведения идентификации состояния ИБ является необходимость четкого посекундного совмещения времени начала маневра с тем, которое имеется в обучающей выборке. Для устранения этого недостатка был проведен повтор-

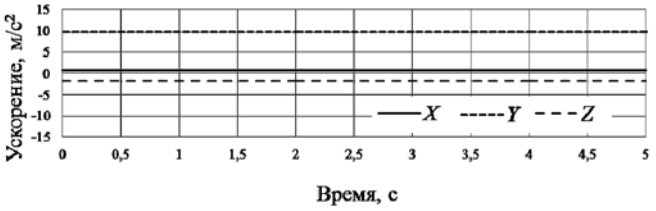

Рис. 5. График проекций ускорения для состояния останова

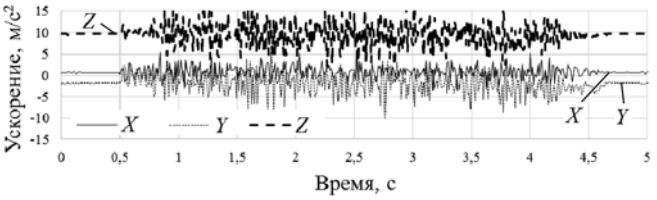

Рис. 6. График проекций ускорения для состояния 1 — "движение прямо"

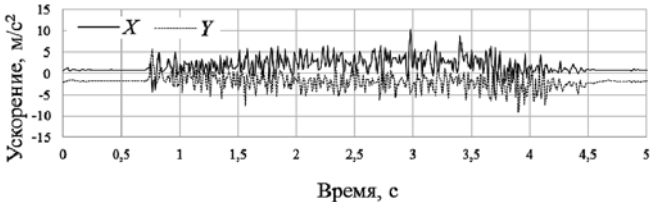

Рис. 7. График проекций ускорения для состояния 2 — "вперед направо"

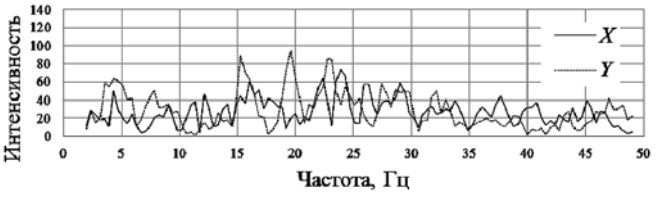

Рис. 8. График спектра ускорения для состояния 1 — "движение прямо"

ный эксперимент с цифровым акселерометром в режиме спектрометра. Для этого к полученным данным был применен алгоритм быстрого преобразования Фурье (FFT). Диапазон частот преобразования Фурье выбирался на основе частоты дискретизации устройства. Для примера приведен график спектра одного из состояний БТС (рис. 8).

4. Результаты эксперимента

Проводилась классификация спектров различных состояний с помощью метода k ближайших соседей (k-NN). В целях оптимизации классификатора имеющийся массив спектральных данных был последовательно проклассифицирован при разных значениях гиперпараметра модели $k = \{2, 3, ..., 15\}$ (рис. 9).

Таким образом, наилучшая точность предложенного классификатора наблюдается при $k = 3$ и уменьшается с увеличением k. В таблице представлены результаты классификации состояния ИБ методом k-NN (при $k = 3$) по шести классам (состояния 1—6).

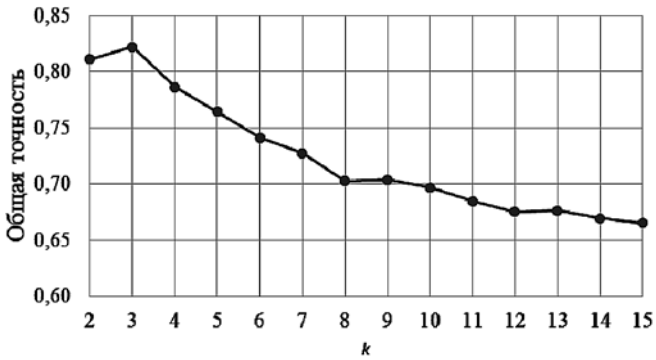

Рис. 9. Зависимость общей точности (overall accuracy) от числа соседних точек (k)

Результаты классификации ИБ методом k-NN ($k = 3$)

Истинный класс	Расчетный класс					
	1	2	3	4	5	6
1	**109 (90,08 %)**	0 (0 %)	5 (4,13 %)	1 (0,83 %)	3 (2,48 %)	3 (2,48 %)
2	3 (2,48 %)	**117 (96,69 %)**	1 (0,83 %)	0 (0 %)	0 (0 %)	0 (0 %)
3	7 (5,79 %)	2 (1,65 %)	**108 (89,26 %)**	1 (0,83 %)	1 (0,83 %)	2 (1,65 %)
4	4 (3,31 %)	1 (0,83 %)	4 (3,31 %)	**104 (85,95 %)**	6 (4,96 %)	2 (1,65 %)
5	16 (13,22 %)	3 (2,48 %)	10 (8,26 %)	10 (8,26 %)	**77 (63,64 %)**	5 (4,13 %)
6	15 (12,40 %)	2 (1,65 %)	11 (9,09 %)	6 (4,96 %)	5 (4,13 %)	**82 (67,77 %)**

Общая точность выбранного классификатора для случая полной классификации составила 0,82. Отдельные классы (состояния 1 и 2) классификатор способен различить с точностью выше 0,9. В то же время наблюдается снижение точности отнесения для отдельных классов (5 и 6), обусловленное сложностью статистического портрета маневров (например, движение вперед-назад). В перспективе с использованием предложенного метода можно значительно повысить точность классификации, применив модель сегментации, описанную авторами в работе [17]. Постоянно сохраняя и обновляя данные о местоположении БТС, можно исключить из рассмотрения маневры, которые невозможны в данный момент времени, и осуществлять классификацию над ограниченным (сегментированным) набором.

Заключение

Показано, что на основе данных внешней контролирующей системы, фиксирующей в режиме реального времени изменение ускорений, возможно с высокой точностью идентифицировать выполняемые БТС маневры, которые в свою очередь зависят от исполняемых на борту информационных процессов и надежности канала связи. В ходе эксперимента общая точность идентификации маневров БТС на основе спектральных данных измерительной системы, составила 0,82.

Достоинствами данного метода является возможность быстрой адаптации моделей состояния, применение различного математического аппарата и методов машинного обучения для получения заданной точности вероятностной оценки. Дальнейшие исследования в данной области могут быть связаны с повышением общей точности идентификации состояний, в частности, путем применения модели сегментации состояний.

Таким образом, предложенный метод является как новой альтернативой, так и дополнением к существующим программным и программно-аппаратным средствам защиты информации и может использоваться для мониторинга ИБ автономных беспилотных объектов. При необходимости и соответствующей настройке контролирующая система может блокировать небезопасные состояния БТС в режиме реального времени.

Список литературы

1. **Semenov V. V., Sukhoparov M. E., Lebedev I. S.** Approach to Side Channel-Based Cybersecurity Monitoring for

Autonomous Unmanned Objects // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2019. Vol. 11659. P. 278—286. DOI: 10.1007/978-3-030-26118-4_27.

2. **Wang M., Huang K., Wang Y., Wu Z., Du Z.** A novel side-channel analysis for physical-domain security in cyber-physical systems // International Journal of Distributed Sensor Networks. 2019. Vol. 15 (8). DOI: 10.1177/1550147719867866.

3. **Devesh M., Kant A. K., Suchit Y. R., Tanuja P., Kumar S. N.** Fruition of CPS and IoT in Context of Industry 4.0 // Choudhury S., Mishra R., Mishra R., Kumar A. (eds) Intelligent Communication, Control and Devices. Advances in Intelligent Systems and Computing. 2020. Vol. 989. P. 367—375. Springer, Singapore. DOI: 10.1007/978-981-13-8618-3_39.

4. **Buldakova T. I.** Cybersecurity Risks Analyses at Remote Monitoring of Object's State // Kravets A., Bolshakov A., Shcherbakov M. (eds) Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control. 2020. Vol 260. Springer, Cham. DOI: 10.1007/978-3-030-32648-7_15.

5. **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.

6. **Faruque M. A., Regazzoni F., Pajic M.** Design methodologies for securing cyber-physical systems // Proceedings of the 2015 international conference on hardware/software codesign and system synthesis (CODES + ISSS), Amsterdam, 4—9 October 2015. New York: IEEE. DOI: 10.1109/CODESISSS.2015.7331365.

7. **Spatz D., Smarra D., Ternovskiy I.** A review of anomaly detection techniques leveraging side-channel emissions // Proceedings of SPIE — The International Society for Optical Engineering. 2019. Vol. 11011 DOI: 10.1117/12.2521450.

8. **Семенов В. В., Лебедев И. С., Сухопаров М. Е.** Идентификация состояния информационной безопасности беспилотных транспортных средств с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации: Матер. 28-й науч.-техн. конф. 24—27 июня 2019 г. 2019. № 28. С. 46—47.

9. **Han Y., Etigowni S., Liu H., Zonouz S., Petropulu A.** Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations // Proceedings of the ACM Conference on Computer and Communications Security. 2017. P. 1095—1108.

10. **Yilmaz B., Prvulovic M., Zajic A.** Electromagnetic Side Channel Information Leakage Created by Execution of Series of Instructions in a Computer Processor // IEEE Transactions on Information Forensics and Security. 2020. Vol. 15. P. 776—789. DOI: 10.1109/TIFS.2019.2929018.

11. **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 (1), P. 73—84. DOI: 10.1007/s10207-018-0403-7.

12. **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.

13. **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.

14. **Семенов В. В., Салахутдинова К. И., Лебедев И. С., Сухопаров М. Е.** Выявление аномальных отклонений при функционировании устройств киберфизических систем // Прикладная информатика. 2019. Т. 14, № 6 (84). С. 114—122. DOI: 10.24411/1993-8314-2019-10053.

15. **Spatz D., Smarra D., Ternovskiy I.** A review of anomaly detection techniques leveraging side-channel emissions // Proc. SPIE 11011, Cyber Sensing. 2019. DOI: 10.1117/12.2521450.

16. **Bishop C. M.** Pattern Recognition and Machine Learning // Information Science and Statistics, Springer, NY, USA. 2006.

17. **Semenov V. V., Lebedev I. S., Sukhoparov M. E., Salakhutdinova K. I.** Application of an Autonomous Object Behavior Model to Classify the Cybersecurity State // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2019. Vol. 11660. P. 104—112. DOI: 10.1007/978-3-030-30859-9_9.

V. V. Semenov, Junior Scientific Researcher, e-mail: v.semenov@iias.spb.su,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
St. Petersburg, Russian Federation

Monitoring of the Information Security State of Unmanned Vehicles by Using Digital Accelerometer

The problem of determining the information security state of an unmanned vehicle by an external monitoring system was considered. The effectiveness of solving this problem is estimated by the overall accuracy of the classification of the state of the object. A method based on the analysis and classification of spectral data recorded by a digital three-axis accelerometer mounted on board a vehicle was proposed. An experiment aimed at studying the proposed method was described. As a result of the experiment, the fundamental possibility of using accelerometer in information security monitoring systems is shown. The overall accuracy of the selected classifier based on the k-NN algorithm was 0.82.

Keywords: *information security, unmanned vehicles, information security monitoring systems, side channels, accelerometer, multivariate data processing*

DOI: 10.17587/it.26.424-430

References

1. **Semenov V. V., Sukhoparov M. E., Lebedev I. S.** Approach to Side Channel-Based Cybersecurity Monitoring for Autonomous Unmanned Objects, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11659, pp. 278-286. DOI: 10.1007/978-3-030-26118-4_27.

2. **Wang M., Huang K., Wang Y., Wu Z., Du Z.** A novel side-channel analysis for physical-domain security in cyber-physical

systems, *International Journal of Distributed Sensor Networks*, 2019, vol. 15 (8). DOI: 10.1177/1550147719867866.

3. **Devesh M., Kant A. K., Suchit Y. R., Tanuja P., Kumar S. N.** Fruition of CPS and IoT in Context of Industry 4.0, Choudhury S., Mishra R., Mishra R., Kumar A. (eds), *Intelligent Communication, Control and Devices. Advances in Intelligent Systems and Computing*, 2020, vol. 989, pp. 367—375. Springer, Singapore. DOI: 10.1007/978-981-13-8618-3_39.

4. **Buldakova T. I.** Cybersecurity Risks Analyses at Remote Monitoring of Object's State, Kravets A., Bolshakov A., Shcherbakov M. (eds), *Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control*, 2020, vol 260. Springer, Cham. DOI: 10.1007/978-3-030-32648-7_15.

5. **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.

6. **Faruque M. A., Regazzoni F., Pajic M.** Design methodologies for securing cyber-physical systems, *Proceedings of the 2015 international conference on hardware/software codesign and system synthesis (CODES + ISSS), Amsterdam, 4—9 October 2015*, New York, IEEE, DOI: 10.1109/CODESISSS.2015.7331365.

7. **Spatz D., Smarra D., Ternovskiy I.** A review of anomaly detection techniques leveraging side-channel emissions, *Proceedings of SPIE — The International Society for Optical Engineering*, 2019, vol. 11011, DOI: 10.1117/12.2521450.

8. **Semenov V. V., Lebedev I. S., Sukhoparov M. E.** Identification of the information security state of unmanned vehicles using artificial neural networks, *Proceedings of the 28th Technical Science Conference "Methods and technical means of ensuring the security of information". June 24—27, 2019 St. Petersburg. Publisher Polytechnic University*, 2019, pp. 46—47 (in Russian).

9. **Han Y., Etigowni S., Liu H., Zonouz S., Petropulu A.** Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations, *Proceedings of the ACM Conference on Computer and Communications Security*, 2017, pp. 1095—1108.

10. **Yilmaz B., Prvulovic M., Zajic A.** Electromagnetic Side Channel Information Leakage Created by Execution of Series of Instructions in a Computer Processor, *IEEE Transactions on Information Forensics and Security*, 2020, vol. 15, pp. 776—789, DOI: 10.1109/TIFS.2019.2929018.

11. **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 (1), pp. 73-84. DOI: 10.1007/s10207-018-0403-7.

12. **Semenov V., Lebedev I., Sukhoparov M.** Identification of the state of individual elements of cyber-physical systems based on external behavioral characteristics, *Prikladnaya informatika — Journal of Applied Informatics*, 2018, vol. 13, no. 5 (77), pp. 72—83 (in Russian).

13. **Semenov V., Lebedev I., Sukhoparov M.** 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.

14. **Semenov V. V., Salakhutdinova K. I., Lebedev I., Sukhoparov M.** Identification of abnormal functioning during the operation devices of cyber-physical systems, *Prikladnaya informatika — Journal of Applied Informatics*, 2019, vol. 14, no. 6(84), pp. 114—122 (in Russian), DOI: 10.24411/1993-8314-2019-10053.

15. **Spatz D., Smarra D., Ternovskiy I.** A review of anomaly detection techniques leveraging side-channel emissions, *Proc. SPIE 11011, Cyber Sensing*, 2019, DOI: 10.1117/12.2521450.

16. **Bishop C. M.** Pattern Recognition and Machine Learning, Information Science and Statistics, *Springer*, NY, USA, 2006.

17. **Semenov V. V., Lebedev I. S., Sukhoparov M. E., Salakhutdinova K. I.** Application of an Autonomous Object Behavior Model to Classify the Cybersecurity State, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11660, pp. 104—112, DOI: 10.1007/978-3-030-30859-9_9.

УДК 004.051 DOI: 10.17587/it.26.430-440

Л. Е. Мистров, д-р техн. наук, проф., e-mail: mistrov_le@mail.ru,
Центральный филиал Российского государственного университета правосудия, г. Воронеж,
Е. В. Головченко, канд. техн. наук, ст. преп., e-mail: evvigo@mail.ru,
Военный учебно-научный центр Военно-воздушных сил "Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина", г. Воронеж

Методологические основы оценки устойчивости функционирования авиационной информационной системы

Показана взаимообусловленная связь между конфликтной устойчивостью авиационных организационно-технических систем и обеспечивающих их применение инфокоммуникационных сетей. Предложен новый показатель устойчивости функционирования авиационных инфокоммуникационных сетей, основанный на положениях теории вероятностей и позволяющий определить нижнюю оценку конфликтной устойчивости авиационных организационно-технических систем.

Ключевые слова: *устойчивость функционирования, эффективность функционирования, авиационные инфокоммуникационные сети, риск, пропускная способность*

Введение

В настоящее время развитие воздушного транспорта сдерживается множеством различных причин. Основные из них можно выразить в виде объективного противоречия: с одной стороны, увеличение объемов воздушных перевозок грузов и пассажиров необходимо