Раздел II. Прикладные вопросы информационной безопасности

УДК 004.075 DOI 10.23683/2311-3103-2017-5-38-47

Д.А. Беспалов, А.А. Ананьев

СПОСОБ ОБНАРУЖЕНИЯ АНОМАЛИЙ В РАБОТЕ ИНФОРМАЦИОННЫХ СИСТЕМ, ИСПОЛЬЗУЮЩИХ ПЛАСТИКОВЫЕ КАРТЫ*

В настоящее время все более актуальной становится проблема анализа поведения сложных информационных систем в реальном времени. В связи с этим в данной статье предлагается способ определения аномалий в поведении информационных систем, использующих интеллектуальные пластиковые карты на основе методов мультифрактального анализа. Решение поставленной задачи базируется на оценке естественного поведение информационных систем, в основе которого лежит фрактальность, то есть самоподобие. При этом под самоподобием системы понимается присутствие повторяемости элементов поведения на фоне общей динамики развития системы. При этом оценка состояния системы проводится по ряду параметров, представленных в виде временных рядов, а обнаружение аномалий поведения выражается в виде артефактов данных временных рядов, нарушающих нормальное протекание процессов. Самоподобие здесь выражается в повторяемости форм временных рядов, в которые любые аномалии вносят свои изменения. При этом, в работе авторов делается упор на информационные системы, в составе которых применяются интеллектуальные пластиковые карты. С одной стороны, пластиковые карты служат элементом, повышающим защищенность системы, тогда как с другой стороны, вносят свои уязвимости как на программном, так и на аппаратном уровне. Вместе с ними в поведении системы появляются артефакты или аномалии, характерные только для пластиковых карт, что затрудняет применение других классических методов детектирования ненормального поведения систем. В отличие от классических методов обнаружения аномалий в данной работе применяется метод, основанный на мультифрактальном анализе, который позволяет проводить мониторинг целевой информационной системы в реальном времени и определять момент наступления аномалии поведения или выделить этап приближения к этому моменту.

Аномалия поведения; анализ; пластиковая карта; информационная система; мультифрактал.

D.A. Bespalov, A.A. Ananev

METHOD FOR DETECTING ANOMALIES IN THE INFORMATION SYSTEMS PERFORMANCE USING PLASTIC CARDS

At present, the problem of analyzing the behavior of complex information systems in real time becomes more urgent. In this regard, this article proposes a method for determining anomalies in the behavior of information systems using intelligent plastic cards based on multifractal analysis methods. The solution of this task is based on an assessment of the natural behavior of information systems, which is based on fractality, that is, self-similarity. In this case, the self-similarity of the system is understood as the presence of the frequency of behavior elements

* Работа выполнена при поддержке ГРАНТа РФФИ 15-07-00595 А.

against the background of the general dynamics of the development of the system. In this case, the evaluation of the state of the system is carried out on a number of parameters represented in the form of time series, and the detection of behavioral anomalies is expressed in the form of artifacts of data of time series that violate the normal course of the processes. Self-similarity here is expressed in the repetition of the forms of time series into which any anomalies make their own changes. At the same time, the authors focus on information systems, which include smart plastic cards. On the one hand, plastic cards serve as an element that increases the security of the system, while on the other hand, they make their vulnerabilities both on a software and hardware level. Together with them in the behavior of the system artefacts or anomalies appear that are characteristic only for plastic cards, which makes it difficult to use other classical methods of detecting abnormal behavior of systems. Unlike the classical methods of detecting anomalies, this work uses a method based on multifractal analysis that allows monitoring the target information system in real time and determining the moment of occurrence of a behavioral anomaly or identifying the stage of approaching this moment.

Anomaly of behavior; analysis; plastic card; information system; multifractal.

Введение. Обнаружение аномалий в поведении информационных систем (ИС) и в протекающих в них процессах является актуальной задачей. Основной целью выявления аномалий поведения ИС представляется обнаружение известных и новых атак на вычислительные ресурсы.

В этой связи, разработка и внедрение новых способов обнаружения, а значит и предупреждения атак на информационные системы указанного вида является актуальной задачей, требующей пристального внимания специалистов в области информационной безопасности.

Постановка задачи. В общем случае аномалии поведения, возникающие в работе информационной системы, использующей микропроцессорные или интеллектуальные пластиковые карты (ИПК) можно классифицировать следующим образом (рис. 1) [6].

Рис. 1. Классификация аномалий

Здесь также следует заметить, что ИС, использующие пластиковые карты имеют более высокую сложность, чем стандартные системы, даже использующие отдельные механизмы, повторяющие функции пластиковых карт (идентификация пользователя, парольная защита, цифровая подпись и т.п.). С одной стороны, пластиковая карты повышает уровень защищенности ИС, с другой стороны, она привносит новые типы уязвимостей в систему [7]. Появление новых видов уязвимостей может быть вызвано как случайными, так и запланированными событиями, например аппаратный сбой, подмена карты или атака по сторонним каналам [8]. Эта сторона вопроса безопасности информационных систем слабо рассмотрена в современных исследованиях.

Анализ защищенности информационной системы, в данном случае, может быть основан на обнаружении аномалий в ее поведении [9].

Далее рассмотрим общее описание способа обнаружения аномалий и диаграмму действий подобной ситуации.

Общее описание способа и диаграмма действий. На сегодняшний день наибольшее распространение получили два класса методов обнаружения аномалий поведения ИС, возникающих в следствие преднамеренного или случайного воздействия, исходящего изнутри системы или из-за ее пределов:

1. Сигнатурные методы обнаружения.
2. Поведенческие методы обнаружения.

Сигнатурные методы обнаружения основываются на гипотезе высокой вероятности выявления ранее известных и формально описанных типов воздействий. Этот класс методов имеет существенный недостаток – они не позволяют уверенно обнаруживать существенные модификации известных воздействий, а тем более – выделять новые типы последних. В современных, динамически развивающихся системах подобные решения являются малоэффективными.

Поведенческие методы обнаружения основываются на выявлении отклонений от штатных режимов функционирования информационных систем, выраженных в изменении значений отдельных параметров или в изменении их статистических характеристик.

Реже встречаются методы, построенные чисто на обнаружении искажений эталонной профильной информации или искажении закономерностей нормального поведения системы. Такие методы сложно применять на практике, так как они малочувствительны к последовательностям возникновения сходных событий, их необходимо отдельно обучать для распознавания ситуаций, когда вредоносное программное обеспечение генерирует последовательности данных, соответствующих нормальному поведению системы.

Следовательно, поставленные задачи можно решать только при помощи универсальных методов, использующих нетрадиционные подходы, например, фрактальные [10–14], бионические, нейросетевые и т.п.

При этом, обобщенную модель поведения при анализе защищенности системы можно выразить в виде нескольких этапов:

1. Мониторинг критических параметров информационной системы и их регистрация.
2. Анализ полученных данных.
3. Поэтапная оценка показателя Херста [15] на различных масштабах.
4. Анализ сингулярности сигнала и локализация аномалий [16–17].
5. Оценка рисков и уровня защищенности системы.

В общем виде, последовательность действий (рис. 2) может быть выражена следующей диаграммой.

Исходя из анализа открытых источников [1] и основываясь на проводимых экспериментах, можно выделить три основных типа измерений для информационных систем, использующих пластиковые карты:

1. Показатели активности – хорошо оценивают вероятность появления аномалии, связанной с резким ускорением работы различных компонент системы. Например, резкий рост числа пакетов между компонентами операционной системы ЭВМ или сторонними программами и драйвером пластиковой карты может свидетельствовать о попытке сканирования содержимого ИПК или о попытке подбора паролей.
2. Измерение категорий – распределение активности программных или аппаратных компонент ИС по некоторым группам. Например, относительная частота попыток входа на некоторый ресурс с использованием транзакций пластиковой карты.
3. Порядковые измерения – используются для оценки различных типов активности, которые могут быть измерены в числовых значениях. Например, число предъявлений PIN-кода карты, число обращений к карте в секунду, число вызовов подпрограммы ИПК со стороны ЭВМ.

Одним из основных моментов в процессе обнаружения аномалий поведения информационной системы и анализе ее защищенности является выбор параметров для обработки. В некоторых случаях сложно изначально определить такой набор параметров – необходим дополнительный анализ или применение отдельных процедур принятия решений.

Далее рассмотрим критерии выбора измерений показателей ИС для дальнейшего анализа.

Рис. 2. Диаграмма действий

Рассмотрим далее критерии оценки защищенности информационных систем, использующих пластиковые карты.

Критерии оценки защищенности. Для выбора конкретного количества измерений показателей анализируемой системы в данной работе использовалась статистика Байеса.

В данном случае, анализировалось множество измерений (1)

$$\{A_{1,}A_2, \dots, A_n\} \quad (1)$$

которые могут быть использованы для определения факта воздействия на информационную систему. Каждое измерение A_i оценивает свой аспект работы системы, например число авторизаций на пластиковой карте за единицу времени. Пусть каждое измерение будет иметь только два значения: 1 (аномальное значение измерения) и 0 (нормальное значение измерения).

Тогда существует гипотеза I того, что к информационной системе было применено воздействие на ее механизмы безопасности.

Достоверность и чувствительность каждого измерения будет определяться соответствующими показателями (2)

$$P(A_j = 1|I) \text{ и } P(A_j = 1|\neg I\ ). \quad (2)$$

Тогда вероятность можно вычислить при помощи теоремы Байеса (3).

$$P(I|A_1, A_2, \dots, A_n) = P(A_1, A_2, \dots, A_n|I)\frac{P(I)}{P(A_1,A_2,\dots,A_n)} \quad (3)$$

Для событий системы I и $\neg I$, вероятно, будет необходимо вычислить условную вероятность для всех возможных сочетаний множества измерений параметров информационной системы. Число условных вероятностей растет экспоненциально по отношению к количеству измерений.

Для сокращения вычислений можно предположить, что каждое измерение A_j зависит только от I и условно не зависит от других измерений из оцениваемого множества.

Тогда (4)

$$P(A_1, A_2, \dots, A_n|I) = \prod_{i=1}^{n} P(A_i|I), \quad (4)$$

и (5)

$$P(A_1, A_2, \dots, A_n|\neg I = \prod_{i=1}^{n} P(A_i|\neg I)). \quad (5)$$

Теперь можно определять вероятность воздействия, используя значения измерений аномалии, вероятности воздействий, произошедших ранее и вероятности появления каждого из измерений аномальной активности, которые были определены ранее во время вторжений.

После проведения экспериментов по каждому типу измерений можно определить ограниченное множество обрабатываемых событий для каждой конкретной информационной системы, использующей пластиковые карты.

Сбор параметров информационной системы, например, мониторинг трафика обмена данными, регистрация вычислительной нагрузки и других подобных показателей является стандартной задачей и в данной работе отдельно рассматриваться не будет.

Поэтому, рассмотрим далее решение задачи анализа полученных данных и их специализированной обработки.

Решение задачи обнаружения аномалий. Можно утверждать, что аномалия в поведении информационной системы, использующей пластиковые карты проявляется либо в существенном изменении некоторых характеристик трафика, либо в появлении или исчезновении характерных пакетов. В любом случае, аномалии проявляются либо стихийно вследствие ошибок, либо периодически в результате запланированной атаки.

Для обнаружения аномалий в работе ИС в данной работе предлагается метод, основывающийся на мультифрактальном анализе или, другими словами, на свойствах самоподобия временных рядов [18, 19].

Современные исследования показали, что информационные процессы, протекающие в системах и выраженные в сетевом трафике или в динамике использования вычислительных и аппаратных ресурсов, имеют свойства самоподобия или, иными словами, свойства фрактальности [20]. Это позволяет использовать теоретический аппарат фрактального анализа для анализа поведения технических систем и для обнаружения воздействий на их элементы.

Под самоподобием здесь понимается повторяемость распределения нагрузки во времени при рассмотрении на различных масштабах и повторяемость типовых кадров данных, генерируемых при работе с устройствами определенного класса.

Величины отдельных параметров информационных систем, изменяющиеся во времени, могут рассматриваться как временные ряды. При этом все изменения регистрируются в определенном масштабе времени, то есть образуют регулярную сетку, фактически, с амплитудами некоторого сигнала или значениями некоторой функции.

При этом, в рассматриваемых рядах значений присутствуют как периодически повторяющиеся элементы, так и асимметрии и эксцессы. Кроме того, можно утверждать, что графики имеют черты самоподобия, то есть обладают фрактальными свойствами. С этой точки зрения можно взглянуть на проблему обнаружения аномалий в информационных системах по-новому.

Для определения уровня стохастичности показателей работы информационной системы можно использовать так называемый показатель Херста [2].

Показатель Херста дает две важные характеристики временного ряда. Во-первых «память системы», которая позволяет оценить инертность движения параметра в условиях случайных или намеренных воздействий, а во-вторых, показатель Херста является устойчивым, то есть содержит минимальное предположение об изучаемой системе, но может идентифицировать вид временного ряда.

Анализ поведения временного ряда в терминах теории фракталов базируется на понятии особой размерности *D*, также называемой «фрактальной».

В общем случае, фрактальная размерность множества Хаусдорфа-Безиковича определяется как (6):

$$D = -\lim_{\varepsilon \to 0} \frac{\lg [N(\varepsilon)]}{\lg [\varepsilon]}, \quad (6)$$

где $N(\varepsilon)$ – это минимальное число непустых каркасов размером ε, покрывающих заданное множество. Фрактальная размерность звязана с показателем Херста H следующим соотношением (7):

$$D = 2 - H \text{ [2]}. \quad (7)$$

Показатель Херста характеризует степень самоподобия данного процесса и может быть определен в следующих трех стабильных диапазонах [3]:

1. $0 < H < 0.5$. Это признак случайного процесса, когда временной ряд является антиперсистентным, т.е. для него характерна и достаточно вероятна смена предыдущего направления движения. Такие значения ряда иногда называют «розовым шумом». Самоподибие ряда здесь слабое и наиболее часто встречаются средние значения величин.
2. $H = 0.5$. Это полностью случайный процесс без ярко выраженной тенденции. В некоторых источниках такой временной ряд называется «белым шумом».

3. *0.5 < H < 1*. Это, так называемый, трендоустойчивый процесс, являющийся персистентным и обладающий длительной памятью. Вцелом является самоподобным, обладает определенной направленностью и часто называется «черным шумом».

При этом, в последнем случае, если ряд возрастает (убывает) в предыдущий период, то весьма вероятно, что он сохранит эту тенденцию на какое-то время в будущем. Тренд в этом случае очевиден. Устойчивость тренда временного ряда или сила персистентности увеличивается при приближении показателя *H* к единице.

Херст в своих работах показал, что большинство естественных явлений соответствует некоторому тренду с шумом и появление стабильных явлений вцелом степенью превышения величиной *H* значения *0.5*.

Для нахождения фрактальной размерности временного ряда можно применить *R/S* анализ [4]. Тогда (8):

$$M\left[\frac{R(n)}{S(n)}\right] \sim cn^H \; при \; n \to \infty, \tag{8}$$

где *n* – число значений временного ряда, *c* – положительная константа, не зависящая от *n*, *H* – показатель Херста, а $R(n)$ – размах временного ряда.

При этом будет справедливо (9–12):

$$R(n) = \max_{1 \le j \le n} \Delta_j - \min_{1 \le j \le n} \Delta_j, \tag{9}$$

$$\Delta_k = \sum_{i=1}^{n} x_i - k\bar{x}, k = \overline{1,n}, \tag{10}$$

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i, \tag{11}$$

$$S(n) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2. \tag{12}$$

Также, по значению *R/S* можно выполнить оценку величины показателя Херста *H* как отношение логарифмов (13):

$$H = \frac{\log\left(\frac{R}{S}\right)}{\log\left(\frac{n}{2}\right)}. \tag{13}$$

Важным свойством предложенного способа определения аномалий является то, что анализ данных ведется на основании нескольких масштабов представления: в долгосрочном, среднесрочном и в краткосрочном периодах. Этот подход обладает определенными преимуществами, например, предсказанная тенденция аномальной активности в долгосрочном периоде может быть рассмотрена более подробно в краткосрочном периоде при увеличении масштаба рассмотрения.

При этом показатели Херста вычисляются для всех собираемых метрик и если они выходят за пределы значений, определенных для нормального поведения, фиксируется состояние ожидания аномалии и вероятного нарушения защищенности информационной системы. Уровень риска в этом случае определяется путем экспертной оценки с точки зрения допустимых пределов безопасности ИС.

Тогда, кроме обнаружения изменений в поведении информационной системы, описываемом в терминах временных рядов, важной задачей является оценка сингулярности временного ряда, позволяющая локализовать аномалии, предсказанные на более крупных масштабах.

Временные ряды, полученные, например, на основе протоколов передачи данных или на основе информации о вычислительной нагрузке системы, имеют эффект самоподобия вследствие особенностей передачи данных, которые приходят на сетевое оборудование разделенными во времени пакетами, а не сплошным потоком или в случайные моменты времени.

Например, трафик беспроводных сетей имеет ярко выраженный всплесковый характер с пульсациями в отдельные моменты времени.

В этом случае, данный тип анализа временных рядов оцениваемых показателей информационных систем основывается на формализации различия спектров с аномалиями и без аномалий путем сравнения фрактальной размерности D_f и корреляционной размерности D_c. Корреляционная размерность выполняется на вычислении корреляционного интеграла, имеющего в своей основе функцию (14)

$$C(\delta) = \frac{1}{n^2}\sum \varepsilon\left(\delta - \left|y_i - y_j\right|\right), \quad (14)$$

где выполняется (15)

$$\varepsilon(x) = \begin{cases} 0, при\ x \le 0 \\ 1, при\ x > 0 \end{cases} \quad (15)$$

функция Хевисайда для всех пар значений i и j, определяющая величину расстояния между точками двух множеств. Если зависимость величины суммы от δ имеет степенной вид (16)

$$C(\delta) \sim \delta^{Dc}, \quad (16)$$

то исследуемое множество фрактально и D_c является его корреляционной размерностью. Для практического расчета можно выделить область линейной зависимости на графике (17)

$$\ln\left(C(\delta)\right) = f(\ln(\delta)) \quad (17)$$

и аппроксимировать функцию прямой линией методом наименьших квадратов [5].

По своей сути, размерности D_f различных вариантов временных рядов отличаются на небольшую постоянную величину и практически не зависят от уровня декомпозиции в базисе вейвлет-функций. Этот вывод логичен, так как выполнение направленных воздействий на информационную систему порождает изменение структуры протекающих в ней процессов, влияет на их свойства самоподобия, что может быть использовано для эффективного обнаружения атак.

На практике сначала должны быть проанализированы временные ряды, получаемые на основе показателей деятельности информационной системы в нормальном режиме без проведения воздействий. В результате этого, получается ряд значений показателя Херста, соответствующий эталонным значениям.

Естественно, что чем качественнее данные, используемые для расчета показателя Херста, тем выше вероятность правильного обнаружения аномалии в работе информационной системы, использующей ИПК.

Для этого целесообразно использовать дополнительные методы обработки временных рядов, выражающих величины анализируемых параметров ИС.

Заключение. В данной работе предложен способ обнаружения аномалий в работе информационной системы, использующей интеллектуальные пластиковые карты на основе методов мультифрактального анализа, позволяющий динамически отслеживать поведение ИС, определяя моменты появления событий, приводящих к последующей атаке на систему со стороны.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Denning D.* An Intrusion Detection Model // IEEE Transactions on Software Engineering. – 1987. – Vol. SE-13, No. I. – P. 222-232.
2. *Калуш Ю.А., Логинов В.М.* Показатель Хёрста и его скрытые свойства // Сибирский журнал индустриальной математики. – 2002. – Т. 5. – Вып. 4. – С. 29-37.
3. *Ляпунова Е.А., Петрова А.Н., Бродова И.Г., Наймарк О.Б., Соковиков М.А., Чудинов В.В., Уваров С.В.* Исследование морфологии многомасштабных дефектных структур и локализации пластической деформации при пробивании мишеней из сплава А6061 // Письма в ЖЭТФ. – 2012. – Т. 38. – Вып. 1. – С. 13-20.
4. *Шелухин О.И., Смольский С.М., Осин А.В.* Самоподобие и фракталы. Телекоммуникационные приложения. – М.: Физматлит, 2008. – 368 с.
5. *Захаров В.С.* Поиск детерминизма в наблюдаемых геолого-геофизических данных: анализ корреляционной размерности временных рядов // Современные процессы геологии: Сборник научных трудов. – М.: Научный мир, 2002. – С. 184-187.

6. *Бабенко Л.К., Беспалов Д.А., Макаревич О.Б.* Современные интеллектуальные пластиковые карты. – М.: Гелиос АРВ, 2015. – 416 с.
7. *Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Трубников Я.А.* Программный комплекс для анализа уязвимостей современных микропроцессорных пластиковых карт // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). – 2014. – С. 576-580.
8. *Беспалов Д.А., Марченко Е.А., Трубников Я.А.* Аппаратный комплекс для анализа устойчивости микропроцессорных систем к воздействиям по сторонним каналам // Информационные технологии, системный анализ и управление (ИТСАиУ-2014): Сборник трудов XII Всероссийской научной конференции молодых ученых, аспирантов и студентов, г. Таганрог, 18-19 декабря 2014 г. – Ростов-на-Дону: Изд-во ЮФУ, 2015. – Т. 1. – С. 90-94.
9. *Babenko Ludmila, Makarevich Oleg, Bespalov Dmitry, Chesnokov Roman, Trubnikov Yaroslav*. Instrumental System for Analysis of Information Systems Using Smart Cards Protection // SIN '14 Proceedings of the 7th International Conference on Security of Information and Networks. ACM New York, NY, USA ©2014. Glasgow, Scotland, UK – September 09-11, 2014. – 339 p.
10. *Lopes R.; Betrouni N*. Fractal and multifractal analysis: A review // Medical Image Analysis. – 2009. – No. 13 (4). – P. 634-649.
11. *Roberts A.J. and Cronin A*. Unbiased estimation of multi-fractal dimensions of finite data sets // Physica A. – 1996. – Vol. 233. – P. 867-878.
12. *Hollestelle G.; Burgers W.; Hartog J*. Power analysis on smartcard algorithms using simulation. Eindhoven, University of Technology. 2004. 40.
13. *Posadas A.N.D., Giménez D., Bittelli, M., Vaz C.M.P., Flury M*. Multifractal Characterization of Soil Particle-Size Distributions // Soil Science Society of America Journal. – 2001. – Vol. 65 (5). – 1361 p.
14. *Hassan M.K., Hassan M.Z., Pavel N.I.* Scale-free network topology and multifractality in a weighted planar stochastic lattice // New Journal of Physics. 12: 093045.
15. *Калуш Ю.А., Логинов В.М.* Показатель Хёрста и его скрытые свойства // Сибирский журнал индустриальной математики. – 2002. – Т. 5. – Вып. 4. – С. 29-37.
16. *Мандельброт Б.Б.* Фракталы, случай и финансы. Регулярная и хаотическая динамика. – Ижевск: Регулярная и хаотическая динамика, 2004. – 256 с.
17. *Falconer K.* Fractal Geometry: Mathematical Foundations and Applications. – 3rd ed. Wiley. 2014. – 398 p.
18. *Albert C. J. Luo*. Toward Analytical Chaos in Nonlinear Systems. Wiley. 2014. – 268 p.
19. *Robert Gilmore, Marc Lefranc*. The Topology of Chaos: Alice in Stretch and Squeezeland. – 2nd ed. Wiley. 2011. – 618 p.
20. *Jianbo Gao, Yinhe Cao, Wen-wen Tung, Jing Hu*. Multiscale Analysis of Complex Time Series: Integration of Chaos and Random Fractal Theory, and Beyond. 2007. – 368 p.

REFERENCRS

1. *Denning D.* An Intrusion Detection Model, *IEEE Transactions on Software Engineering*, 1987, Vol. SE-13, No. I, pp. 222-232.
2. *Kalush Yu.A., Loginov V.M.* Pokazatel' Khersta i ego skrytye svoystva [The Hurst exponent and its hidden properties], *Sibirskiy zhurnal industrial'noy matematiki* [Siberian journal of industrial mathematics], 2002, Vol. 5, Issue 4, pp. 29-37.
3. *Lyapunova E.A., Petrova A.N., Brodova I.G., Naymark O.B., Sokovikov M.A., Chudinov V.V., Uvarov S.V.* Issledovanie morfologii mnogomasshtabnykh defektnykh struktur i lokalizatsii plasticheskoy deformatsii pri probivanii misheney iz splava A6061 [The study of the morphology of multiscale defect structures and localization of plastic deformation during the penetration of targets from alloy A6061], *Pis'ma v ZhETF* [JETP Letters], 2012, Vol. 38, Issue 1, pp. 13-20.
4. *Shelukhin O.I., Smol'skiy S.M., Osin A.V.* Samopodobie i fraktaly. Telekommunikatsionnye prilozheniya [Self-similarity and fractals. Telecommunication application]. Moscow: Fizmatlit, 2008, 368 p.
5. *Zakharov V.S.* Poisk determinizma v nablyudaemykh geologo-geofizicheskikh dannykh: analiz korrelyatsionnoy razmernosti vremennykh ryadov [The search for determinism in observed geological and geophysical data: the analysis of correlation dimensions of time series], *Sovremennye protsessy geologii: Sbornik nauchnykh trudov* [Modern processes Geology: Collection of scientific works]. Moscow: Nauchnyy mir, 2002, pp. 184-187.

6. *Babenko L.K., Bespalov D.A., Makarevich O.B.* Sovremennye intellektual'nye plastikovye karty [Modern intellectual plastic cards]. Moscow: Gelios ARV, 2015, 416 p.
7. *Babenko L.K., Bespalov D.A., Makarevich O.B., Trubnikov Ya.A.* Programmnyy kompleks dlya analiza uyazvimostey sovremennykh mikroprotsessornykh plastikovykh kart [A software package for the analysis of vulnerabilities of modern microprocessor plastic cards], *Materialy konferentsii «Informatsionnye tekhnologii v upravlenii» (ITU-2014)* [Materials of conference "Information technologies in management" (IUT-2014)], 2014, pp. 576-580.
8. *Bespalov D.A., Marchenko E.A., Trubnikov Ya.A.* Apparatnyy kompleks dlya analiza ustoychivosti mikroprotsessornykh sistem k vozdeystviyam po storonnim kanalam [Hardware for stability analysis of microprocessor systems to the impacts on third-party channels], *Informatsionnye tekhnologii, sistemnyy analiz i upravlenie (ITSAiU-2014): Sbornik trudov XII Vserossiyskoy nauchnoy konferentsii molodykh uchenykh, aspirantov i studentov, g. Taganrog, 18-19 dekabrya 2014 g*. [Information technology, system analysis and management (Idayu-2014): proceedings of the XII all-Russian scientific conference of young scientists, postgraduates and students, Taganrog, 18-19 December 2014]. Rostov-na-Donu: Izd-vo YuFU, 2015, Vol. 1, pp. 90-94.
9. *Babenko Ludmila, Makarevich Oleg, Bespalov Dmitry, Chesnokov Roman, Trubnikov Yaroslav*. Instrumental System for Analysis of Information Systems Using Smart Cards Protection, *SIN '14 Proceedings of the 7th International Conference on Security of Information and Networks. ACM New York, NY, USA ©2014. Glasgow, Scotland, UK – September 09-11, 2014*, 339 p.
10. *Lopes R., Betrouni N*. Fractal and multifractal analysis: A review, *Medical Image Analysis*, 2009, No. 13 (4), pp. 634-649.
11. *Roberts A.J. and Cronin A*. Unbiased estimation of multi-fractal dimensions of finite data sets, *Physica A*, 1996, Vol. 233, pp. 867-878.
12. *Hollestelle G.; Burgers W.; Hartog J*. Power analysis on smartcard algorithms using simulation. Eindhoven, University of Technology. 2004. 40.
13. *Posadas A.N.D., Giménez D., Bittelli, M., Vaz C.M.P., Flury M*. Multifractal Characterization of Soil Particle-Size Distributions, *Soil Science Society of America Journal*, 2001, Vol. 65 (5), 1361 p.
14. *Hassan M.K., Hassan M.Z., Pavel N.I.* Scale-free network topology and multifractality in a weighted planar stochastic lattice, *New Journal of Physics*. 12: 093045.
15. *Kalush Yu.A., Loginov V.M.* Pokazatel' Khersta i ego skrytye svoystva [The Hurst exponent and its hidden properties], *Sibirskiy zhurnal industrial'noy matematiki* [Siberian journal of industrial mathematics], 2002, Vol. 5, Issue 4, pp. 29-37.
16. *Mandel'brot B.B.* Fraktaly, sluchay i finansy. Regulyarnaya i khaoticheskaya dinamika [Fractals, occasion and finances. Regular and chaotic dynamics]. Izhevsk: Regulyarnaya i khaoticheskaya dinamika, 2004, 256 p.
17. *Falconer K.* Fractal Geometry: Mathematical Foundations and Applications. 3rd ed. Wiley. 2014, 398 p.
18. *Albert C. J. Luo*. Toward Analytical Chaos in Nonlinear Systems. Wiley. 2014, 268 p.
19. *Robert Gilmore, Marc Lefranc*. The Topology of Chaos: Alice in Stretch and Squeezeland. 2nd ed. Wiley. 2011, 618 p.
20. *Jianbo Gao, Yinhe Cao, Wen-wen Tung, Jing Hu*. Multiscale Analysis of Complex Time Series: Integration of Chaos and Random Fractal Theory, and Beyond. 2007, 368 p.

Статью рекомендовал к опубликованию д.т.н. Н.И. Витиска.

Беспалов Дмитрий Анатольевич – Южный федеральный университет; e-mail: bda82@mail.ru; 347928, г. Таганрог, ул. Чехова, 2, корп. «И»; тел.: 89604661762; кафедра вычислительной техники; доцент.

Ананьев Александр Александрович – e-mail: a.ananev@outlook.com; тел.: 89094396586; кафедра безопасности информационных технологий; аспирант.

Bespalov Dmitry Anatolyevich – Southern Federal University; e-mail: bda82@mail.ru; 2, Chekhov street, build. "I", Taganrog, 347928, Russia; phone: +79604661762; the department of computer science; associate professor.

Ananev Alexander Alexandrovich – e-mail: a.ananev@outlook.com; phone: +79094396586; the department of information technology security; postgraduate student.