Вісник Національного технічного університету "ХПІ", 2018, № 42 (1318)
ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

УДК 004.732.056 **DOI: 10.20998/2411-0558.2018.42.05**

С. Ю. ГАВРИЛЕНКО, канд. техн. наук, проф., НТУ "ХПИ",
В. В. ЧЕЛАК, магистр, НТУ "ХПИ",
В. В. ДАВЫДОВ, канд. техн. наук, доц., НТУ "ХПИ"

РАЗРАБОТКА СИСТЕМЫ ФИКСАЦИИ АНОМАЛЬНЫХ СОСТОЯНИЙ КОМПЬЮТЕРА

Предложена система фиксации аномальных состояний компьютера на базе нечеткой логики. В качестве входных данных модели использованы шаблоны нормального состояния компьютерной системы, базирующиеся на контрольных картах, BDS-статистике, показателе Херста и качественных метриках. Выполнена оптимизация системы и проведено ее тестирование, которое показало, что вероятность обнаружения аномальной работы компьютерной системы с учетом ложных срабатываний достигает 96,5%. Результаты исследований показали возможность использования разработанного модуля в эвристических анализаторах систем обнаружения вторжений. Ил.: 5. Библиогр.: 19 назв.

Ключевые слова: аномальное состояние, антивирусная защита информации; BDS-статистика; контрольные карты; показатель Херста; системы обнаружения вторжений; эвристический анализатор.

Постановка проблемы. Новые информационные технологии успешно внедряются во все сферы человеческой деятельности и являются самой большой ценностью современного общества. С ростом ценности информации вырос и спрос на неё, и вместе с этим – количество желающих получить к ней несанкционированный доступ за счет использования компьютерных вирусов. Указанная проблема усиливается распространением Интернет-технологий, переходом на облачные технологии и динамическим ростом количества мобильных устройств. Все это приводит к росту количества вредоносного программного обеспечения (ВПО). Несмотря на принятые во многих странах законы по борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Поэтому актуальной темой является разработка эффективных методов и технологий противостояния компьютерным вирусам, что позволит своевременно обнаружить аномальное состояние компьютерной системы и предотвратит возможные катастрофические последствия.

Анализ литературы [1, 2] показал, что современные антивирусные программы не могут обеспечить полную защиту компьютерных систем (КС). Это обусловлено тем, что принципы анализа ВПО не могут обнаружить новые версии вредоносных программ до их анализа

аналитиками антивирусных компаний, и внесения сигнатур вновь созданных вирусов в антивирусные базы данных. Использование различных эвристических моделей оценки состояния объекта по результатам измерений контролируемых показателей и базирующихся на различных методах, также имеет ряд недостатков.

Так использование многофакторных дискриминантных моделей [3] зависит от особенностей контролируемых показателей, их смысла, объема, что приводит к низкой точности и скорости, высокой вероятности ложных срабатываний.

Кластерный анализ [4, 5] достаточно прост в реализации, имеет однозначную трактовку результатов. Вместе с тем, принадлежность к какому-либо кластеру не всегда информативна, так как не учитывается близость точек к границам разделения на кластеры.

Мощным, эффективным методом является регрессионный анализ [6], позволяющий учесть также взаимодействие между выбранными показателями. Вместе с тем данному методу присуще жесткость механизма преобразования исходных данных в конечный результат, субъективный характер выбора вида конкретной зависимости (формальная подгонка модели под эмпирический материал), невозможность объяснения причинно-следственной связи [7 – 9] и, как следствие, недостаточная информативность результатов, что допускает неоднозначную их трактовку.

Дисперсионный анализ позволяет проверить наличие влияния взаимодействия факторов, но вместе с тем он чувствителен к нарушениям условий нормальности и гомоскедастичности.

Системы обнаружения аномального состояния системы также плохо адаптированы для обработки больших объемов данных в режиме реального времени [10, 11].

Данные недостатки трудно устранить, используя только классические методы обнаружения ВПО. Одним из путей увеличения эффективности систем компьютерной безопасности является аргументированный выбор критериев оценки аномального поведения КС.

В условиях воздействия на компьютерную систему ВПО изменяются показатели функционирования компьютерной системы (загрузка центрального процессора, оперативной памяти, траффика и т.д.), что зачастую приводит к сбоям в работе аппаратного и программного обеспечения. Проведенные исследования показали эффективность использования различных статистических методов обработки вышеперечисленных показателей функционирования системы для оценки состояния компьютера [12 – 17].

В данной работе в качестве входных данных разрабатываемой модели фиксации аномального состояния компьютерной системы (сканера) использованы ранее полученные нами результаты исследований: значения BDS-теста в статике и динамике [12, 13], показатель Херста [14], контрольные карты Шухарта (ККШ), карты кумулятивных сумм (КУСУМ), карты EMWA [15, 16] и Парето, а также качественные метрики, полученные посредством анализа PE-структуры файла и действий, выполняемых вредоносным программным обеспечением [17].

BDS-тест основан на статистической величине:

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1}\,\frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}, \qquad (1)$$

где $w_{m,N}(\varepsilon)$ – значение BDS-статистики; N – число элементов временного ряда; $C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m$ – числитель *BDS*-статистики, определяющийся корреляционными интегралами $C_{m,N}(\varepsilon)$; $C_{1,N-m}(\varepsilon)^m$ для выборки размера m; ε – радиус гиперсферы; $\sigma_{m,N}(\varepsilon)$ – среднеквадратичное отклонение разницы $C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m$.

Ранее нами получено [12, 13], что критерием оценки нормального состояния компьютерной системы для входных данных является значение джиттера BDS-теста в интервале [25%, 75%].

Показатель Херста характеризует степень самоподобия процесса. Предыдущие исследования показали [14], что влияние ряда вирусов на компьютерную систему приводит к изменению показателя Херста, который характеризуется стремлением к среднему значению 0,55, что указывает на случайность процесса, то есть процесс не является самоподобным.

Известно, что ККШ карты обнаруживают значительные и краткосрочные изменения процесса, карты КУСУМ – с большой вероятностью обнаруживают небольшие, но постоянные изменения, карты EWMA позволяют выполнять мониторинг полной истории выходных значений. Использование разных типов контрольных карт позволяет более точно оценить состояние компьютерной системы. Экспериментальные данные позволили построить шаблоны нормального состояния компьютерной системы, выход за рамки которых свидетельствует об аномальности [15, 16]. Признаком аномального состояние компьютерной системы также является:

– для контрольных карт Шухарта – наличие 7 и более точек подряд выше средней границы;

– для КУСУМ-карт – резкое изменение угла наклона графика.

Последний входной критерий предложенной системы базируется на результатах анализа PE-структуры файла [17]. По результатам анализа 6000 экземпляров ВПО (типа Worm, Backdoor, Trojan) найдено множество признаков, присущих этим файлам. 20 из них выделено для дальнейшего анализа, а именно: удаление антивирусных программ и программ мониторинга; отключение диспетчера задач; удаление файлов антивирусных баз; отключение загрузки компьютера в защищенном режиме; закрытие программ, в заголовках которых содержаться строки, указывающие на принадлежность к антивирусному программному обеспечению; отключение User Account Control (компоненты и технологии безопасности Microsoft Windows); отключение брандмауэр Windows; запрет редактирования реестра; регистрация и запуск службы для блокировки доступа к сайтам антивирусных компаний; остановка службы и выгрузка из памяти процессов, относящихся к антивирусным программам и Firewall и др.

Для определения коэффициента значимости анализируемых признаков, случайным образом выбрано 40 вредоносных файлов, получены бинарные вектора каждого образца. Для дальнейшего использования качественные метрики, оценены с помощью аппарата линейного программирования с целевой функцией (2) и ограничениями (3), (4):

$$Z = x_1 + x_2 + \ldots + x_n \rightarrow \max, \tag{2}$$

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n \geq K_a, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2n}x_n \geq K_a, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{m1}x_1 + b_{m2}x_2 + \ldots + b_{mn}x_n \geq K_a, \end{cases} \tag{3}$$

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n \leq K_b, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2n}x_n \leq K_b, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{m1}x_1 + b_{m2}x_2 + \ldots + b_{mn}x_n \leq K_b, \end{cases} \tag{4}$$

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

где x_i $(i = 1, 2, \mathbf{L}, n)$ – коэффициент значимости *i*-го признака, b_{ij} $(i = 1, 2, \ldots, n, \quad j = 1, 2, \ldots, m)$ – бинарные коэффициенты, означающие присутствие или отсутствие *i*-го признака в *j*-ом образце, K_a, K_b начало и конец диапазона допустимых значений выборки.

Цель статьи – разработка, исследование и совершенствование методов и моделей фиксации аномальных состояний компьютерных систем.

Результаты разработки сканера обнаружения вторжений в компьютерные системы. Так как часть входных данных имеет интервальный характер, то было принято решение в основе работы сканера использовать аппарат нечеткой логики [18, 19]. Кроме того, в отличие от традиционных математических задач, которые, требуют на каждом шаге моделирования однозначной формулировки закономерностей, нечеткая логика является совершенно иным уровнем мышления, при котором постулируется лишь минимальный набор закономерностей, благодаря которому творческий процесс моделирования происходит на наивысшем уровне абстракции. Она позволяет быстро моделировать сложные динамические системы и сравнивать их с заданной степенью точности.

Процесс нечеткого вывода представляет собой некоторую процедуру, или алгоритм получения нечетких выводов на основе нечетких условий или предпосылок. Этот процесс сочетает в себе все основные концепции теории нечетких множеств, функций принадлежности, лингвистических переменных, нечетких логических операций, методов нечеткой импликации и нечеткой композиции.

Структурная схема сканера приведена на рис. 1.

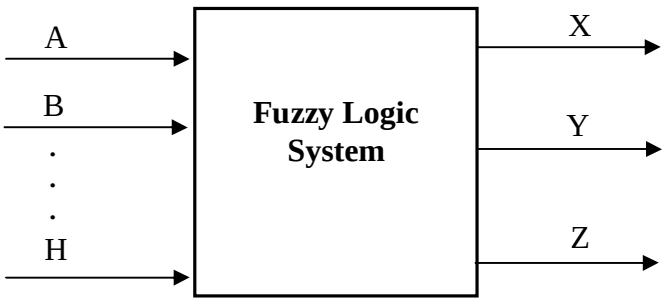

Рис. 1. Структурная схема системы фиксации аномального состояния компьютера

На рис. 1 приняты следующие обозначения: *A* – значение BDS-теста; *B* – значение контрольных карт Шухарта; *C* – значение карт CUSUM; *D* – значение EWMA-карт; *E* – значение показателя Хертста; *F* – значение качественной метрики (QM); *G* – значение BDS-теста виртуальной машины; *H* – значение карт Парето; *X* – активация подпрограммы "Лечение"; *Y* – активация подпрограммы "Удаление"; *Z* – активация подпрограммы "Карантин".

Активация выходных подпрограмм задана следующим образом. Если значение *X* или *Y*, или *Z* больше либо равно 0.75, запускается соответствующая подпрограмма. В случае срабатывания нескольких выходов приоритет вызова подпрограмм следующий: "Лечение" (*X*), Карантин (*Z*), Удаление (*Y*).

Входные лингвистические переменные для системы нечеткого вывода по методу Мамдани описаны таким кортежем:

$$< \alpha, T, L, G_r, M>,$$

где: α – имя лингвистической переменной (*A*, *B*, *C*, *D*, *E*, *F*, *G*, *H*); *T* – множество значений (термов) входной лингвистической переменной {"Опасный", "Возможно опасный", "Неопределенный", "Безопасный", "Скорее безопасный"}; *L* – множество отградуированных значений входной переменной; G_r – процедура агрегации условий (новых термов); *M* – функция формирования нечеткого множества значений для каждого терма заданной лингвистической переменной.

Экспериментальные данные позволили определить для каждой из входных и выходных переменных количество, тип и значение функций принадлежности. Тестирование предложенной системы проводилось в пакете Matlab. Как видно из рис. 2, входная переменная *A* (значение BDS-теста) задана 5 функциями принадлежности: *Z*-образный, трапециевидный, треугольный и *S*-образный типы. Форма и границы функций принадлежности выбраны на основе экспериментальных данных.

Входные и выходные лингвистические переменные связываются базой правил. Фрагмент базы правил приведен на рис. 3, где темным цветом выделено правило нахождения объекта для нормального состояния. Предварительный расчет количества правил (произведение числа нечетких множеств всех входных переменных) показал, что число правил равно 45000, что является существенным недостатком данного метода. Для уменьшения количества правил принято решение выполнить попарное сравнение нечетких переменных. В результате получено 443 правила. Для более корректной работы, база правил дополнена 44 правилами для двух краевых ситуаций (срабатывают от 8 – 9 краевых

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

функций принадлежности) и 30 правилами для противоречивых ситуаций. В итоге получено 517 правил, что существенно увеличило быстродействие предложенной системы.

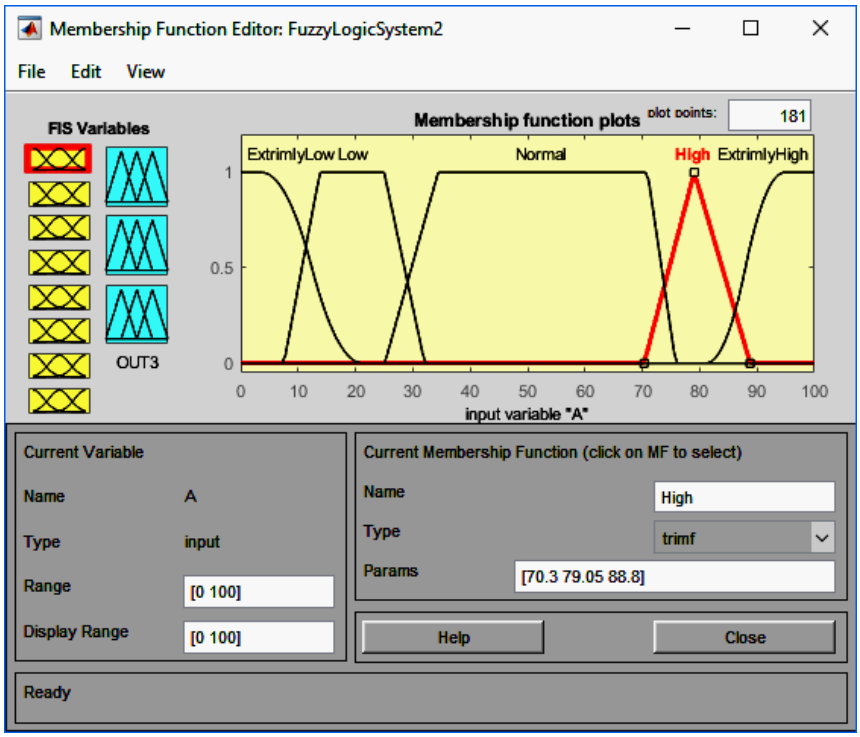

Рис.2. График функции принадлежности входной лингвистической переменной *A* (значение BDS теста)

В дальнейшем, для решения задачи, система нечеткого вывода принимает решение на основе весовых коэффициентов каждого из подусловий правила, и, опираясь на сложившуюся базу правил, дает определенный нечеткий вывод. Субъективная исходная оценка далее проходит процесс дефаззификации, то есть процесс перехода от функции принадлежности выходной лингвистической переменной к ее четкому числовому значению [18]. Процесс дефаззификации может проводиться различными методами, например, методом центра тяжести:

$$\Delta = \int_{\min}^{\max} xMF(x)dx \Big/ \int_{\min}^{\max} MF(x)dx \qquad (5)$$

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

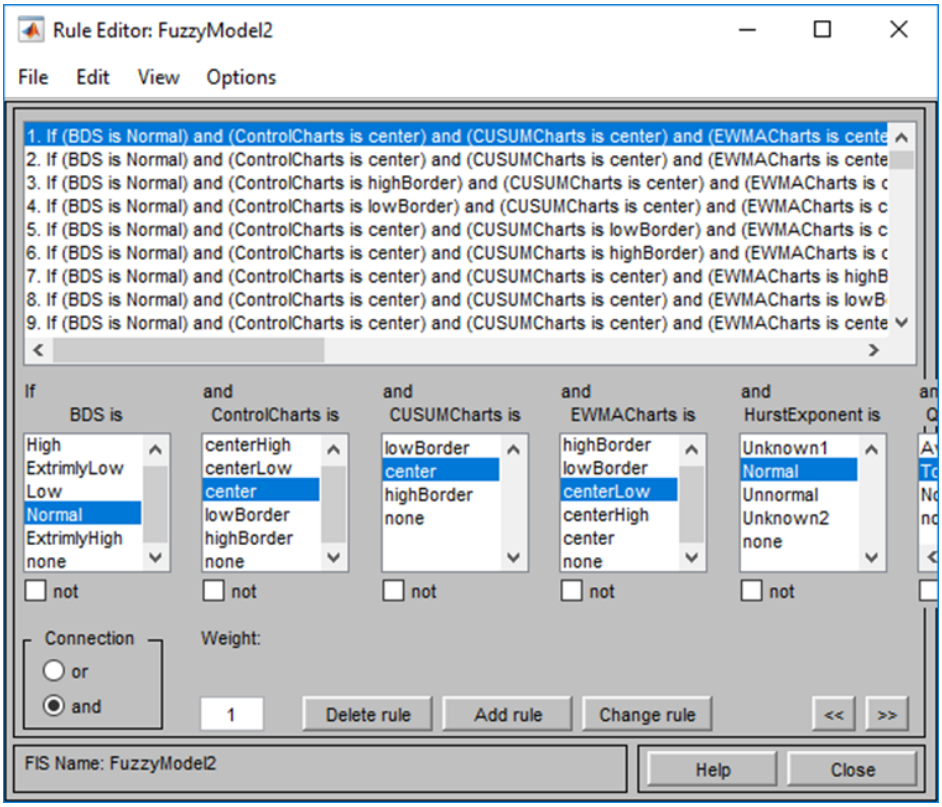

Рис. 3. Фрагмент базы правил системы нечеткого вывода

Фрагмент результатов фиксации аномального состояния системы с наихудшими показателями входных параметров приведен рис. 4.

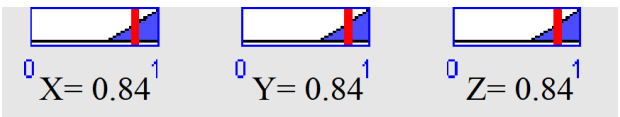

Рис. 4. Результат фиксации аномального состояния системы

На вход поданы следующие параметры компьютерной системы: значение BDS-теста – 0, значение контрольных карт Шухарта – 50, значение карт CUSUM – 50, значение EWMA-карт – 50, значение показателя Хертста 55, качественной метрики (QM) – 30, значение BDS-теста виртуальной машины – 0, значение карт Парето – 100. Получены следующие выходные значения: X = 0,84; Y = 0,84; Z = 0,84. Согласно ранее разработанной базе правил, такой результат свидетельствует об аномальности компьютерной системы. Как результат, выполнится

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

активации программы "Лечение". В случае отрицательного результата подпрограммы, активируется подпрограмма "Карантин". В худшем случае, будет активирована подпрограмма "Удаление", которая деактивирует вредоносное ПО и удалит все данные, которые были связаны с ним (данные реестра, ОЗУ, файлы, скрипты установки и т.п.).

Обобщенные результаты эксперимента приведены на рис. 5. Всего использовалось 4 типа ВПО, процесс распознавания длился 500 с. Как видно из графика в течении 500 с было обнаружено около 96,5% вредоносного программного обеспечения с учетом ложных срабатываний.

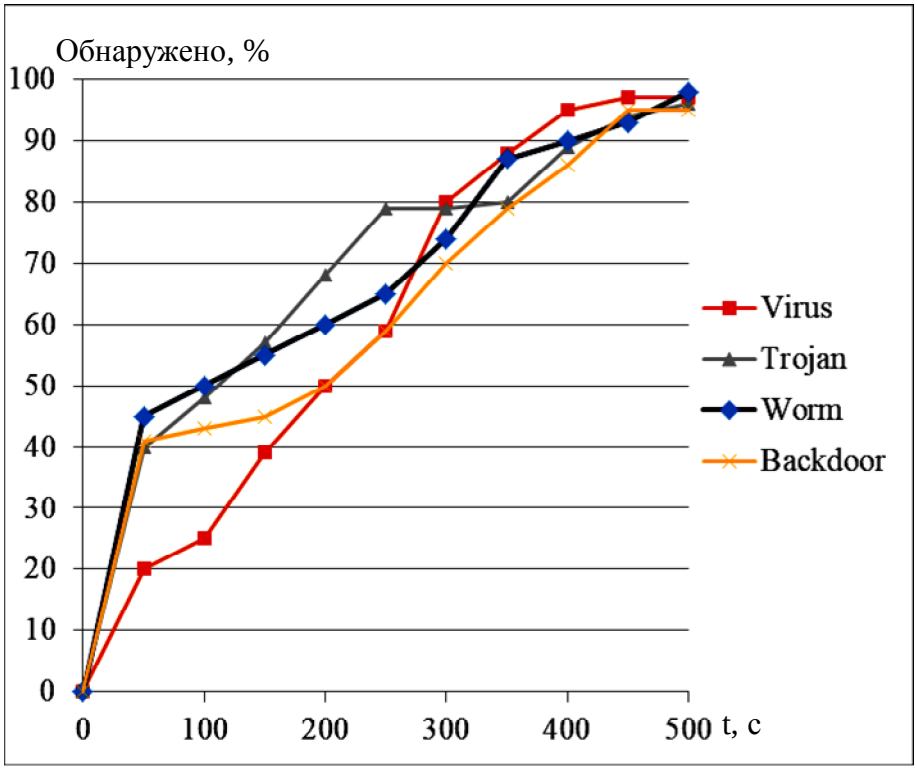

Рис. 5. Результаты тестирования системы

Выводы. В работе проведено сравнительное исследование основных методов оценки состояний компьютерных систем, показаны их преимущества и недостатки. Предложена система фиксации аномального состояния компьютера.

Впервые, в качестве входных данных системы использованы критерии, полученные и апробированные в предыдущих исследованиях:

шаблоны нормального состояния КС, базирующиеся на контрольных картах, BDS-статистике, показателе Херста и качественных метриках.

В основе работы системы использовано аппарат нечеткой логики. Выполнена оптимизация работы предложенной системы за счет уменьшения количества правил, связывающих входные и выходные нечеткие переменные, что позволило увеличить ее быстродействие.

Проведено тестирование разработанной системы, которое показало, что вероятность обнаружения ВПО, с учетом ложных срабатываний, составляет 96.5%.

Полученные результаты исследований показали, что предложенная система фиксации аномального состояния компьютера позволяет строить многоуровневые нечеткие продукционные модели, а используемый механизм нечеткого вывода на основе алгоритма Мамдани (Mamdani) позволяет принять решение и выработать меры по предотвращению катастрофических последствий.

Список литературы:

1. *Семенов С.Г.* Защита данных в компьютеризированных управляющих системах (монография) / *С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко* // "LAP LAMBERT ACADEMIC PUBLISHING": Germany, 2014. – 236 с.

2. *Шелухин О.И.* Обнаружение вторжений в компьютерные сети / *О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова.* – М.: Горячая линия-Телеком, 2013. – 220 с.

3. *Illowsky Barbara.* Introductory Statistics / *Barbara Illowsky, Susan Dean.* – OpenStax CNX, 2014. – 905 p.

4. *Everitt Brian*. Cluster analysis / *Brian Everitt.* – Chichester, West Sussex, U.K: Wiley, 2011. – 330 p.

5. *Суслов С.А.* Кластерный анализ: сущность, преимущества и недостатки / *С.А. Суслов* // Вестник НГИЭИ. – 2010. – Vol. 1. – № 1. – С. 51-57.

6. *Sen A.* Regression Analysis – Theory, Methods, and Applications / *A. Sen, M. Srivastava.* – Springer-Verlag, Berlin, 2011. – 264 p.

7. *Nugzar Todua*. ANOVA in marketing research of consumer behavior of different categories in georgian market / *Todua Nugzar, Dotchviri Teona* // Annals of the Constantin Brancusi University of Targu Jiu. – Economy Series. – 2015. – Issue 1. – Vol. I. – P. 183-189.

8. *Weedmark David.* The Advantages & Disadvantages of a Multiple Regression Model. – Sciencing. – 2018. https://sciencing.com/advantages-disadvantages-multiple-regression-model-12070171.html.

9. *Flom Peter*. The Disadvantages of Linear Regression. – Sciencing, 2018, https://sciencing.com/disadvantages-linear-regression-8562780.html.

10. *Лукацкий А.В.* Обнаружение атак. – СПб.: BXB-Петербург, 2001. – 624 с.

11. *Касперский К.* Играй, как "Лаборатория Касперского": компания открывает доступ к своей базе знаний о киберугрозах в рамках нового бизнес-сервиса – Режим доступа: https://www.kaspersky.ru/about/press-releases/2017_kompaniya-otkryvayet-dostup-k-svoyey-baze-znaniy-o-kiberugrozakh-v-ramkakh-novogo-biznes-servisa

12. *Семенов С.Г.* Разработка шаблонов идентификации состояния компьютерных систем на основе BDS-тестирования / *С.Г. Семенов, С.Ю. Гавриленко, В.В. Челак* // Вісник НТУ

"ХПІ". Серія "Інформатика та моделювання". – Харків: НТУ "ХПІ", 2016.– № 21. – С. 118-125.
13. *Semenov S.* Developing parametrical criterion for registering abnormal behavior in computer and telecommunication systems on the basis of economic test // *S. Semenov, S. Gavrilenko, V. Chelak* //Actual problems of economics. – Kiev, 2016. – Vol 4 (178). – P. 451-459.
14. *Gavrylenko S.* Investigation of intrusion in computer systems based on the hurst exponent / *S. Gavrylenko. V. Chelak, N. Bilogorskiy* // Advanced Information System. Quarterly scientific and technical journal. – Kharkiv: KhPI, 2017. – Vol. 1. – № 2. – P. 58-61.
15. *Gavrylenko S.* Intrusion detection in computer systems / *S. Gavrilenko, V. Chelak, O. Hornostal* // Proceedings of the symposium "Metrology and metrology assurance". – Sozopol, Bulgaria, 2016. – P. 342-347.
16. *Гавриленко С.Ю.* Разработка адаптивных шаблонов фиксации аномального поведения компьютерной системы / *С.Г. Семенов, С.Ю. Гавриленко, А.А. Горносталь* // Зб. наукових праць. Системи обробки інформації. – Х.: ХУ ПС, 2016. – № 3 (140). – С. 11-14.
17. *Gavrylenko S.* Development of the method and program model of the static analyzer of harmful files / *S. Gavrylenko and D. Saenko* // Advanced Information System. Quarterly scientific and technical journal. – Kharkiv: KhPI, 2017. – Vol. 1. – № 1. – P.44-48.
18. *Gavrylenko S.* Development of a heuristic antivirus scanner based on the file's PE-structure analysis / *S.Yu. Gavrylenko, M.S. Melnyk, V.V. Chelak* // Інформаційні технології та комп'ютерна інженерія. Міжнародний науково-технічний журнал.– Вінниця: ВНТУ, 2017. – №3 (40). – С. 23-29.
19. *Зайченко Ю.П.* Нечеткие модели и методы в интеллектуальных системах / *Ю.П. Зайченко*. – К.: Слово, 2008. – 344 с.

References:

1. Semenov, S., Davydov, V. and Gavrilenko, S. (2014), *Data Protection in Computer-Aided Control Systems*, "LAP LAMBERT ACADEMIC PUBLISHING", Germany, 236 p.
2. Shelukhin, O.I., Sakalema, D.Zh. and Filinova, A.S. (2013), *Detection of intrusions into computer networks*. Hot line-Telecom, Moscow, 220 p.
3. Illowsky, Barbara, Dean, Susan (2014), *Introductory Statistics*, OpenStax CNX, 905 p.
4. Everitt, Brian (2011), *Cluster analysis*, Chichester, West Sussex, U.K: Wiley, 330 p.
5. Suslov, S.A. (2010), "Cluster analysis: the nature, advantages and disadvantages", *Vestnik NGIEI*, Vol. 1, No. 1, pp. 51-57.
6. Sen, A., Srivastava, M. (2011), *Regression Analysis – Theory, Methods, and Applications*, Springer-Verlag, Berlin, 264 p.
7. Nugzar, Todua and Teona, Dotchviri (2015), "ANOVA in marketing research of consumer behavior of different categories in georgian market", *Annals of the "Constantin Brancusi" University of Targu Jiu*, Economy Series, Issue 1, Vol. I, pp 183-189.
8. Weedmark, David (2018), *The Advantages & Disadvantages of a Multiple Regression Model*. Sciencing, available at: https://sciencing.com/advantages-disadvantages-multiple-regression-model-12070171.html.
9. Flom, Peter (2018), *The Disadvantages of Linear Regression*, Sciencing, available at: https://sciencing.com/disadvantages-linear-regression-8562780.html.
10. Lukatsky, A.V. (2001), *Detection of attacks*, VKhV, St. Petersburg, 624 p.
11. Kaspersky, K. (2017), *Play as Kaspersky Lab: The company opens up access to its knowledge base on cyber threats within a new business service*, available at:

https://www.kaspersky.com/about/press-releases/2017_kompaniya-otkryvayet-dostup-k-svoyey-baz-znaniy-o-cybergrozakh-v-ramkakh-novogo-business-service
12. Semenov, S., Gavrilenko, S. and Chelak, V. (2016), "Development of templates for the identification of the state of computer systems based on BDS-testing", *Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling*, Vol. 21, pp.118-125.
13. Semenov, S., Gavrilenko, S. and Chelak, V. (2016), "Developing parametrical criterion for registering abnormal behavior in computer and telecommunication systems on the basis of economic test", *Actual problems of economics*, Vol 4 (178), pp. 451-459.
14. Gavrylenko, S., Chelak, V. and Bilogorskiy, N. (2017), "Investigation of intrusion in computer systems based on the hurst exponent", *Herald of the National Technical University "KhPI". Subject issue: Advanced Information System*, Volume 1, No. 2, pp.58-61.
15. Gavrilenko, S., Chelak, V., Hornostal, O. (2016), "Intrusion detection in computer systems". *Proceedings of the symposium "Metrology and metrology assurance",* Sozopol, Bulgaria, pp. 342-347.
16. Gavrilenko, S.Yu., Semenov, S.G. and Gornostal, A.A. (2016), "Development of adaptive patterns for fixing anomalous behavior of a computer system", *Herald of the National Technical University "KhPI". Subject issue: Sb. scientific works Systems of information processing,* Vol. 3 (140), pp. 11-14.
17. Gavrylenko, S. and Saenko, D. (2017), "Development of the method and program model of the static analyzer of harmful files", *Herald of the National Technical University "KhPI". Subject issue: Advanced Information System. Quarterly scientific and technical journal*, Vol. 1, No1, pp.44-48.
18. Gavrylenko, S.Yu., Melnyk, M.S. and Chelak, V.V. (2017), "Development of a heuristic antivirus scanner based on the file's PE-structure analysis", *Herald of the Vinnitsa National Technical University. Subject issue: Information Technology and Computer Engineering. International scientific and technical journal,* No. 3 (40), pp. 23-29.
19. Zaychenko, Yu.P. (2008), *Fuzzy Models and Methods in Intellectual Systems*, Word, Kiev, 344 pp.

Статью представил д.т.н., проф. Национального технического университета "Харковский политехнический институт" С.Г. Семенов

Поступила (received) 23.10.2018

Gavrilenko Svetlana, PhD Tech.,
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 21, Kharkov, Ukraine, 61002
Tel: (057) 707-01-65, e-mail: 7573997@gmail.com
ORCID ID: 0000-0002-6919-0055

Chelak Viktor, master
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 21, Kharkov, Ukraine, 61002
Tel: (050) 867-88-55, e-mail: victor.chelak@gmail.com
ORCID ID: 0000-0001-8810-3394

Davydov Viacheslav, PhD Tech.,
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 21, Kharkov, Ukraine, 61002
Tel: (050) 867-88-55, e-mail: vyacheslav.v.davydov@gmail.com
ORCID ID: 0000-0002-2976-8422

УДК 004.732.056

Розробка системи фіксації аномального стану комп'ютера / Гавриленко С.Ю., Челак В.В., Давидов В.В. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2018. – № 42 (1318). – С. 109 – 121.

Представлено систему фіксації аномального стану комп'ютера на базі нечіткої логіки. В якості вхідних даних моделі використані шаблони нормального стану комп'ютерної системи, що базуються на контрольних картах, BDS-статистике, показниках Херста, а також якісних метриках. Виконано оптимізацію системи за рахунок зменшення кількості правил, що дозволило збільшити її швидкість. Проведено тестування розробленої системи, яке показало, що вірогідність виявлення наявності аномальної роботи комп'ютерної системи з урахуванням помилкових спрацьовувань досягає 96,5%. Результати дослідження показали можливість використання розробленого модуля у евристичних аналізаторах систем виявлення вторгнень. Іл.: 5. Бібліогр .: 19 назв.

Ключові слова: аномальне стан; антивірусний захист інформації; BDS-статистика; контрольні карти; показник Херста; системи виявлення вторгнень; евристичний аналізатор.

УДК 004.732.056

Разработка системы фиксации аномальных состояний компьютера / Гавриленко С.Ю., Челак В.В., Давыдов В.В. // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2018. – № 42 (1318). – С. 109 – 121.

Предложена система фиксации аномального состояния компьютера на базе нечеткой логики. В качестве входных данных модели использованы шаблоны нормального состояния компьютерной системы, базирующиеся на контрольных картах, BDS-статистике, показателе Херста и качественных метриках. Выполнена оптимизация системы и проведено тестирование системы, которое показало, что вероятность обнаружения аномальной работы компьютерной системы с учетом ложных срабатываний достигает 96,5%. Результаты исследований показали возможность использования разработанного модуля в эвристических анализаторах систем обнаружения вторжений. Ил.: 5. Библиогр.: 19 назв.

Ключевые слова: аномальное состояние; антивирусная защита информации; BDS-статистика; контрольные карты; показатель Херста; системы обнаружения вторжений; эвристический анализатор.

UDC 004.732.056

Development of a system for fixing a computer's anomalous state / Gavrilenko S.Yu., Chelak V.V., Davydov V.V. // Herald of the National Technical University "KhPI". Series of "Informatics and Modeling". – Kharkov: NTU "KhPI". – 2018. – №.42 (1318). – P. 109 – 121.

The means of anti-virus information protection, their advantages and disadvantages are considered. A system for fixing the anomalous computer state, based on fuzzy logic, is proposed. The models of the normal state of a computer system based on control charts, BDS-statistics, the Hurst index, as well as qualitative metrics, were used as input data of the model. The system was optimized by reducing the number of rules, which made it possible to increase its speed. Testing of the developed system was carried out, which showed that the probability of detecting the presence of abnormal operation of a computer system, taking into account false alarms, reaches 96,5%. The results of the research showed the possibility of using the developed module in heuristic analyzers of intrusion detection systems. Figs.: 5. Bibliography: 19 titles.

Keywords: anomalous state; anti-virus information protection; BDS-statistics; control cards; Hurst indicator; intrusion detection systems; heuristic analyzer.