УДК 004.056

СОВЕРШЕНСТВОВАНИЕ КИБЕРЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ЗА СЧЕТ АДАПТИВНЫХ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ КИБЕРАТАК

Валерий Лахно, Анна Терещук, Тарас Петренко

Развитие информационных систем и технологий, в том числе на критически важных объектах инфраструктуры, вызвал интерес к исследованиям в области проектирования и создания инновационных систем киберзащиты, базирующихся на интеллектуальных адаптивных технологиях обнаружения и распознавания кибервторжений. В условиях роста количества дестабилизирующих воздействий на состояние кибербезопасности критически важных информационных систем (КВІС) необходимы дальнейшие исследования, направленные на развитие методологических и теоретических основ информационного синтеза систем киберзащиты, способных к самообучению. В статье предложена категориальная модель и алгоритм информационно-экстремального обучения адаптивной системы интеллектуального распознавания киберугроз с возможностью комбинирования методологии, основанной на адаптивных сплайнах, и гиперэллипсоидной коррекции решающих правил на основе кластеризации признаков. Объединение двух технологий распознавания в разрабатываемой адаптивной системе киберзащиты позволит минимизировать количество обучающих выборок для идентификации киберугроз, атак и аномалий.

Ключевые слова: *адаптивные системы распознавания, критически важные информационные системы, адаптивные сплайны, кластеризация признаков кибератак.*

Введение. Масштабное развитие компьютерных технологий и критически важных информационных систем (КВИС) в ключевых отраслях экономики требует постоянного отслеживания киберугроз, а также уязвимостей технических компонентов и программного обеспечения информационно-коммуникационных инфраструктур в энергетике, промышленности на транспорте и т.п. Несовершенство существующих технологий выявления вторжений и обнаружения аномалий в КВИС, а также изменяющийся характер действий атакующей стороны, потенциально может способствовать переходу КВИС в небезопасные состояния. Объединение нескольких инновационных технологий выявления угроз, аномалий и кибератак в перспективных адаптивных системах распознавания (АСР) может дать ощутимый эффект в исследованиях, посвященных проблематике обеспечения кибербезопасности КВИС.

Таким образом, одним из перспективных и актуальных направлений исследований систем интеллектуального распознавания киберугроз является предоставление им свойства адаптивности. В частности, при этом можно использовать модели и методы, базирующиеся на методологии адаптивных сплайнов, а также информационно-экстремальную технологию, основанную на максимизации информационной способности АСР.

Анализ литературных данных и постановка проблемы. Проблематике синтеза интеллектуальных систем распознавания угроз, аномалий и кибератак посвящено достаточно большое количество публикаций. В работах [1, 2] авторы делают подробный обзор и анализ существующих методов обнаружения аномалий в компьютерных системах. В работе [3] предложены принципы классификации методов обнаружения, базирующиеся на машинном обучении и статистическом анализе поведения объектов КВИС. Обзор современных методов машинного обучения для систем распознавания кибератак (СРКА) достаточно полно представлен в работах [4–6]. Дальнейшее развитие этих работ прослеживается в публикации [7], посвященной применению метода k–средних, и его модификациям [8-10]. Развитию СРКА на основе применения конечных автоматов (КА) посвящены работы [11, 12]. Другим перспективным направлением развития СРКА является направление, связанное с обнаружения злоупотреблений на основе состояний КВИС [13, 14, 15].

Методы вычислительного интеллекта, в частности, нейронные сети (НС) для задач обнаружения кибератак, описаны в работах [16, 17]. В [13, 18] описаны модели и методы адаптации генетических алгоритмов для задачи обнаружения кибератак. В работах [19, 20] описаны вычислительные иммунные системы, которые можно использовать для задачи построения АСР. Ряд авторов предлагают строить АСР на базе байесовских сетей [21] или MAP-сплайнов [22]. В частности, это позволяет по заданным параметрам строить точную аппроксимацию поведения

обычного пользователя или атакующей стороны.

Однако, многими авторами отмечен типичный недостаток большинства СРКА – ошибочные срабатывания [17, 19, 23]. По мнению авторов работ [8, 15, 21, 24], это связано с задействованием в СРКА одной технологии обнаружения атак. Таким образом, перспективным направлением развития методов обнаружения кибератак и аномалий является объединение существующих подходов в адаптивные гибридные СРКА, обладающие способностью к самообучению.

Постановка цели и задач исследования. Цель исследования – разработка модели и алгоритма обучения двухступенчатой адаптивной системы распознавания, основанной на применении адаптивных сплайнов и нечеткой кластеризации признаков аномалий, киберугроз или кибератак.

Для достижения цели работы необходимо решить следующие задачи:

– разработать модель, которая позволяет для конкретных КВИС устанавливать отношения между элементами АСР;

– разработать алгоритм обучения АСР с использованием на первом этапе адаптивных регрессионных сплайнов, а на втором – процедуры нечеткой кластеризации признаков аномалий или кибератак, а также гиперэллипсоидной коррекции решающих правил.

Модель и алгоритм обучения адаптивной системы распознавания.

Математическое описание АСР выглядит следующим образом:

$$\Delta =< I \times T \times S \times \Omega \times K, X^{|2|}, B^{|2|}, \phi_1, \phi_2 >, \qquad (1)$$

где I – множество входных факторов (сигналов), которые влияют на информационную безопасность (ИБ) КВИС; T – множество моментов времени, в ходе которых происходит снятие параметров «слепков» ИБ; S – пространство признаков объекта распознавания; Ω – пространство возможных функциональных состояний ИБ КВИС; K – база знаний для идентификации аномалий, киберугроз или кибератак; $X^{|2|}$ – учебная матрица (эталон) для двух классов; $B^{|2|}$ – бинарная учебная матрица; ϕ_1, ϕ_2 – операторы формирования входной и бинарной учебных матриц соответственно.

Схематическая модель АСР приведена на рис. 1.

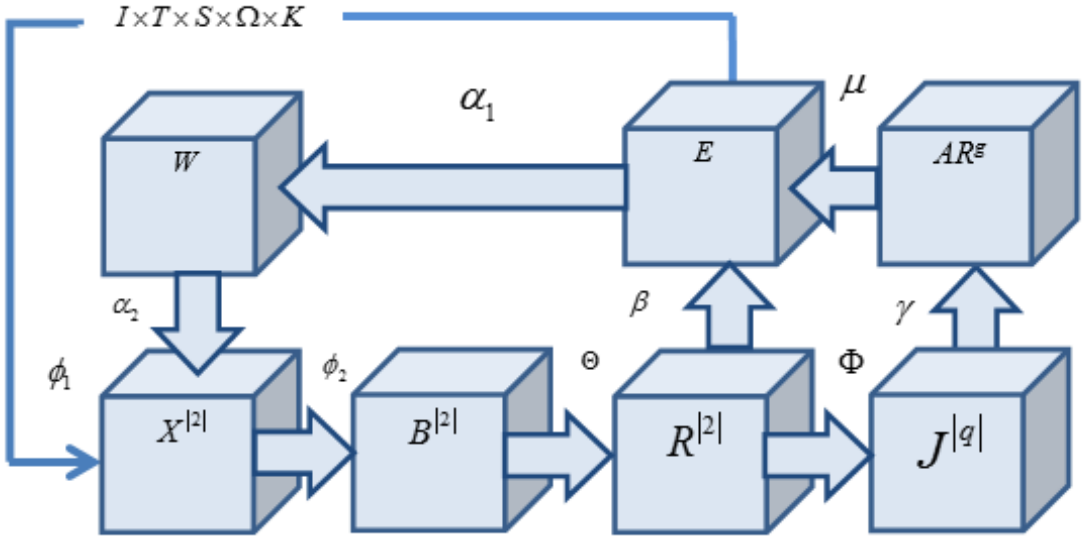

Рис. 1. Схематическая модель АСР для КВИС

Ниже описана последовательность функционирования АСР в формате категориальных составляющих. Оператор $\Theta : B^{|2|} \to R^{|2|}$ позволяет разбить пространство признаков аномалий, киберугроз или кибератак (далее по тексту - объектов) на два класса распознавания. С помощью параметра классификации Φ проверяется статистическая гипотеза о принадлежности реализаций к моделируемому классу объектов, например, для этой процедуры можно использовать адаптивные регрессионные сплайны. Оператор γ формирует множество AR^g, которое характеризует точность распознавания АСР. Примем: q – количество статистических гипотез, $g = q^2$ – количество характеристик АСР. Оператор μ формирует множество E, включающее в себя

значения информационного критерия функциональной эффективности (ИКФЭ) АСР. Оператор β используется для оптимизации системы контрольных отклонений АСР. Множество W последовательно замыкается операторами $\alpha_1 : E \to W$ и $\alpha_2 : W \to X$, которые отслеживают реализацию объектов в процессе обучения АСР.

На первом этапе распознавания объектов в АСР рассмотрим работу оператора классификации Φ. Статистические данные нормальной (или аномальной) активности отображаются в последовательность векторов данного пространства. Задача метода MARS состоит в построении наилучшей аппроксимации поведения по заданной статистике в виде обучающего множества векторов, при этом в качестве аппроксимирующей функции используются многомерные адаптивные регрессионные сплайны. Построение модели MARS происходит в два хода: прямого и обратного. Во время прямого хода критерием добавления вершин в модель есть оптимальность следующего шага. Вершины добавляться до тех пор, пока модель не достигнет максимального уровня сложности. При обратном же ходе малозначимые вершины удаляются из модели, что приводит к ее упрощению. Построенный сплайн является «шаблоном» атаки либо нормального поведения систем.

Пусть задана некоторая выборка $\{x_i; y_i\}$, $i = \overline{1, N}$, при этом зависимость между y_i и x_i можно представить в виде $y_i = f(x_i) + \varepsilon$, где $f(x)$ – неизвестная функция, ε – ошибка приближения.

Алгоритм MARS аппроксимирует прогнозированное значение активности $\tilde{f}$ в виде разложения в ряд по базисным функциям

$$\tilde{f} = \alpha_0 + \sum_{k=1}^{K} \alpha_k F_k(x), \qquad (2)$$

где α_0 – сдвиг модели; K – количество базисных функций; F_k и α_k – k-ая базисная функция и ее коэффициент [23].

Пусть $\delta(y)$ – ступенчатая функция, определяющая положительный аргумент

$$\delta(y) = \begin{cases} 1, & \textit{если} \quad y \ge 0; \\ 0, & \textit{если} \quad y < 0. \end{cases} \qquad (3)$$

В одномерном случае в качестве базисных функций выбирают кусочно-линейные функции вида $\delta\left(\pm (x - z)\right)_+^r$, где z – координата узла; $r \ge 0$ – степень сплайна.

Наипростейшие базисные функции MAR-сплайна порядка $r = 1$ называются рефлексивными парами (*reflected pair*). Часто данные функции представляют в виде

$$(x - z)_+ = \begin{cases} x - z, & \textit{если} \quad x \ge z, \\ 0, & \textit{если} \quad x < z; \end{cases} \qquad (4)$$

$$(z - x)_+ = \begin{cases} z - x, & \textit{если} \quad x \le z, \\ 0, & \textit{если} \quad x > z. \end{cases} \qquad (5)$$

В многомерном случае независимая переменная является вектором $X = (x_1, x_2, ..., x_i, ..., x_s)$. Для каждого значения x_i строятся рефлексивные пары с узлом в точке $z = x_{i,j}$, $i = \overline{1, N}$, $j = \overline{1, s}$. По данным значениям можно построить класс базисных функций $\Psi = \left\{(x_j - z)_+^r; (z - x_j)_+^r\right\}$, $z \in \left\{x_{1,j}; x_{2,j}; ...; x_{N,j}\right\}_{j=1}^{s}$. В результате этого базисная функция F_k определяется уравнением вида

$$F_k(x) = \prod_{l=1}^{N_k} \delta\left[\pm (x_{l,k} - z_{l,k})\right]_+^r, \qquad (6)$$

где N_k – количество функций из класса Ψ, которые входят в k-ую базисную функцию, $x_{l,k}$ – координата вектора X, которая входит в состав l-ой линейной функции k-ой базисной функции, $z_{l,k}$ – узел, который соответствует $x_{l,k}$.

Для построения базисной функции $F_k(x)$ можно использовать не только функции из класса Ψ, но также и функции, производные от них. Для нахождения коэффициентов α_k можно использовать методы минимизации невязки, например, дискретный метод наименьших квадратов.

На втором этапе распознавания реализуется процесс формирования априорно нечеткой классифицированной учебной матрицы с целью построения решающих правил в процессе обучения АСР.

Предположим, что известна априорно неклассифицированная многомерная учебная матрица для АСР $\left\| x_i^{(j)} \right\|$, $i = \overline{1, M}$, $j = \overline{1, m}$, где M, m – соответственно количество признаков распознавания объектов и испытаний.

Постановка задачи:

1) в режиме кластерного анализа необходимо преобразовать входящую неклассифицированную учебную матрицу признаков в нечеткую классифицированную;

2) в режиме обучения построить четкое разбиение пространства признаков распознавания аномалий, киберугроз или кибератак на классы $\{C_n,\ n=\overline{1,N}\}$, которые соответственно характеризируют функциональные состояния управляемого процесса киберзащиты, путем оптимизации координат вектора параметров функционирования системы ИБ для КВИС

$$z =< N, p, \rho, f_{n1}, f_{n2}, S, y_n >, \qquad (7)$$

где N – количество кластеров или мощность алфавита классов распознавания аномалий в работе КВИС или киберугроз; p – показатель нечеткости для алгоритма; ρ – поля допусков на признаки распознавания аномалии, угрозы или атаки; f_{n1}, f_{n2} – двоичные векторы, определяющие координаты первого и второго фокусов гиперэллипсоидного контейнера для класса аномалий, киберугроз (кибератак) в бинарном пространстве признаков S; y_n – полуось контейнера класса в пространстве признаков S. Ограничения на формирование выборки ранее описаны в работе [24].

В процессе обучения АСР определяются координаты вектора параметров терма (7). Это, в свою очередь, позволяет обеспечить значение усредненных по алфавиту классов ИКФЭ распознавания аномалий, угроз или кибератак в КВИС, соответственно:

$$\overline{E} = \frac{1}{N}\sum_{n=11}^{N}\max_{\{h\}} E_n, \qquad (8)$$

где E_n – значение ИКФЭ обучения АСР для реализации класса аномалий или кибератак C_n; $\{h\}$ – множество шагов для обучения АСР.

В режиме тестовой проверки АСР принимается решение о принадлежности реализаций эталонных образов, характеризующих текущее функциональное состояние информационной безопасности, к соответствующему классу С, сформированному на этапе обучения АСР. То есть, на этом этапе выполняется дефазификация нечетких данных $\left\{C_n \middle| n=\overline{1,N}\right\}$.

Инициализация входящих некластеризованных данных о признаках аномалий или кибератак подано в виде (векторной) матрицы $\left\{x_i^j \middle| i=\overline{1,M},\ j=\overline{1,m}\right\}$.

На следующем этапе работы алгоритма генерируются матрицы нечеткого разбиения:

$$U = \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1m} \\ u_{21} & u_{22} & \dots & u_{2m} \\ & \dots & & \\ u_{n1} & u_{n2} & \dots & u_{nm} \end{bmatrix},$$

при условии $u_{nj} \in \{0,1\};\ \sum_{n=1}^{N} u_{nj} = 1;\ 0 < \sum_{n=1}^{N} u_{nj} < m,$

где u_{nj} – степень независимости j-го объекта к кластеру – n.

Расчет центров кластеров признаков аномалий и кибератак осуществляется по следующей формуле:

$$x_n = \frac{\sum_{j=1}^{M}\left(u_{nj}\right)^p \cdot x^{(j)}}{\sum_{j=1}^{M}\left(u_{nj}^{(k-1)}\right)^p}, \qquad (9)$$

где k – счетчик количества итераций.

В результате работы алгоритма минимизируется целевая функция:

$$F = \sum_{n=1}^{N}\sum_{j=1}^{m} u_{nj}^p \cdot y_{\text{cov}}^2\left(x^{(j)}, x_n\right),$$

где y_{cov} – ковариация для кластера n.

В случае необходимости, пересчет элементов матрицы нечеткого разбиения выполняется по следующей формуле:

$$u_{nj}^{(k)} = 1\Bigg/\left[\sum_{h=1}^{N}\left(\frac{y_{\text{cov}}^2\left(x^{(j)}, x_n\right)}{y_{\text{cov}}^2\left(x^{(j)}, x_h\right)}\right)^{\frac{1}{h-1}}\right]. \qquad (10)$$

Проверка модели выполнена для 5 классов кибератак на КВИС: «отказ в обслуживании», «загрузки враждебного ПО», «несанкционированное выполнение команд», «нарушение прав доступа», «несанкционированный доступ к паролю». При этом количество признаков распознавания варьировалось в пределах $M = 9-15$. Оптимальное количество кластеров избиралось по ИКФЭ обучения АСР (рис. 2). Как показал анализ результатов, оптимальное количество кластеров равно $N = 3$.

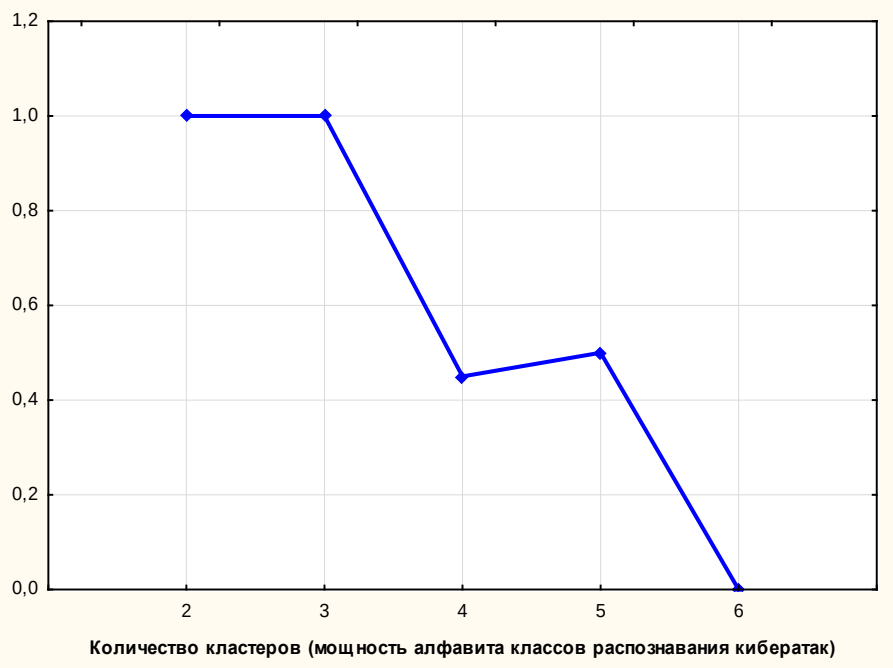

Рис. 2. Оптимальное количество кластеров для max значения ИКФЭ в процессе обучения АСР

В отличие от алгоритмов, используемых для обучения для конечных автоматов [11] и случайного отбора [14], предложенный алгоритм способен автоматически определять размеры учебной и тестовой матриц признаков аномалий, киберугроз или кибератак, не требуя участия экспертов.

Апробация алгоритма осуществлялась только для известных классов аномалий и кибератак. Это является определенным недостатком исследования. Для более сложных кибератак и аномалий, очевидно, потребуется увеличение количества признаков, а также шагов алгоритма обучения АСР $w > 3500$, что повышает уровень требований к вычислительным ресурсам.

Перспективы дальнейших исследований в области синтеза АСР угроз, аномалий и кибератак для КВИС состоят в том, чтобы усовершенствовать базу знаний системы, а также провести исследования на большем количестве классов кибератак на КВИС.

Выводы. В результате выполненных исследований:

– разработана модель, которая позволяет на этапе анализа АСР для конкретных КВИС устанавливать отношения между элементами адаптивных систем киберзащиты;

– разработана модель и алгоритм двухэтапного обучения АСР с возможностью применения на первом этапе адаптивных регрессионных сплайнов, а на втором - процедуры нечеткой кластеризации признаков объектов, а также гиперэллипсоидной коррекции решающих правил, что позволило создать адаптивный механизм самообучения системы распознавания аномалий, угроз и кибератак в КВИС. Во время тестирования алгоритма установлено, что он является наиболее эффективным для трёх кластеров в задачах разбиения пространства признаков объектов. При этом, в режиме тестового обучения АСР, достаточное количество шагов для безошибочного определения классов аномалий, киберугроз или кибератак составляет $h = 2500 - 3000$.

ЛИТЕРАТУРА

[1]. Abidar, R. Intelligent and Pervasive Supervising Platform for Information System Security Based on Multi-Agent Systems [Text] / R. Abidar, K. Moummadi, F. Moutaouakkil, H. Medromi // international review on computers and software. – 2015. – Vol. 10, Issue 1. – p. 44–51.

[2]. Alcaraz, C. Critical Control System Protection in the 21st Century [Text] / C. Alcaraz, S. Zeadally // Computer. – 2013. – vol. 46, Issue 10. – p. 74–83.

[3]. Jegede, A. J. Information Security Policy: Relevance, Creation and Enforce-ment [Text] / A. J. Jegede, G. I. O. Aimufua, H. O. Salami // International Journal of Soft Computing. – 2007. – Vol. 2, Issue 3. – p. 408–410.

[4]. Hassani, A. Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity [Text] / A. A. El Hassani, A. A. El Kalam, A. Bouhoula, R. Abassi, A. A. Ouahman // International Journal of Information Security. – 2015. –Vol. 14, Issue 4. – p. 367–385.

[5]. 2015 Attacks Statistics [Electronic resource]. – Available at: http://www.hackmageddon. com / 2016 / 01/ 11/ 2015-cyber-attacks-statistics.

[6]. Дудикевич В. Б. Проблеми оцінки ефективності систем захисту [Текст] / В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник Національного університету "Львівська політехніка". Сер.: Автоматика, вимірювання та керування. – 2012. – № 741. – С. 118–122.

[7]. Грищук, Р. В. Атаки на інформацію в інформаційно-комунікаційних системах [Текст] / Р. В. Грищук // Сучасна спеціальна техніка. – 2011. – № 1 (24). – С. 61–66.

[8]. Корченко, А. А. Система формирования нечетких эталонов сетевых параметров [Текст] / А. А. Корченко // Захист інформації. – 2013. – Т. 15, № 3. – С. 240–246.

[9]. Lahno, V. Ensuring of information processes' reliability and security in critical application data processing systems [Text] / V. Lahno // MEST Journal. – Belgrade. – 2014. –Vol. 2, Issue 1. – P. 71–79.

[10]. Manap, N. A. Legal Issues of Data Protection in Cloud Computing [Text] / N. Manap, S.Basir, S. Hussein, P. Tehrani, A. Rouhani // International Journal of Soft Computing. – 2013. – Vol. 8, Issue 5. – P. 371–376.

[11]. George, J. A. Improving Authentication and Authorization for Identity Based Cloud Environment Using OAUTH with Fuzzy Based Blowfish Algorithm [Text] / J. A. George, M. Hemalatha // international review on computers and software. – 2015. – Vol. 10, Issue 7. – p. 783–788.

[12]. Li, H.-H. Study of Network Access Control System Featuring Collaboratively Interacting Network Security Components [Text] / H.-H. Li, C.-L. Wu // international review on computers and software. – 2013. – Vol. 8, Issue 2. – P. 527–532.

[13]. Geuna K.Applying Need Pull and Technology Push Theory to Organizational Information Security Management [Text] / K. Geuna, K. Sanghyun // International Business Management. – 2015. – Vol. 9. Issue 4. – p. 524–531.

[14]. Geetha, R. Secure Communication Against Framing Attack in Wireless Sensor Network [Text] / R. Geetha, E. Kannan // international review on computers and software. – 2015. – Vol. 10, Issue 4. – p. 393–398.

[15]. Shamshirband, S. An appraisal and design of a multiagent system based cooperative wireless intrusion detection computational intelligence technique [Text] / S. Shamshirband, N. B. Anuar, M. L. Kiah, A. Patel, // Engineering Applications of Artificial Intelligence. – 2013. – Vol. 26, Issue 9. – p. 2105–2127.

[16]. Мірошник, М. А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах [Текст] / М. А. Мірошник // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – 2015. – № 4 (113). – С. 39–43.

[17]. Keunsoo, L. DDoS attack detection method using cluster analysis [Text] / L. Keunsoo, J. Kim, K. Hoon Kwon, Y. Han, S. Kim // Expert Systems with Applications. – 2008. – Vol. 4, Issue 3. – p. 1659–1665.

[18]. Dilek, S. Applications of artificial intelligence techniques to combating cyber-crimes: A review [Text] / S. Dilek, H. Çakır, M. Aydın // International Journal of Artificial Intelligence & Applications. – 2015. – Vol. 6, Issue 1. – P. 21–39.

[19]. Patel, A. M. An intrusion detection and prevention system in cloud computing: A systematic review [Text] / A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Junior // Journal of Network and Computer Applications. – 2013. – Vol. 36, Issue 1. – P. 25–41.

[20]. Barman, D. K. Design of Intrusion Detection System Based On Artificial Neural Network and Application of Rough Set [Text] / D. K. Barman, G. Khataniar // International Journal of Computer Science and Communication Networks. – 2012. – Vol. 2, Issue 4. – P. 548–552.

[21]. Raiyn, J. A survey of Cyber Attack Detection Strategies [Text] / J. Raiyn // International Journal of Security and Its Applications. – 2014. – Vol. 8, Issue 1 –P. 247–256.

[22]. Mukkamala, S. Intrusion detection systems using adaptive regression splines [Text] / S. Mukkamala, A.H. Sung, A. Abraham, V. Ramos // Sixth International Conference on Enterprise Information Systems. – 2006. – Part 3. – P. 211–218.

[23]. Kotenko, I. Integrated repository of security information for network security evaluation [Text] / I. Kotenko, A. Fedorchenko, A. Chechulin // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). – 2015. – Vol. 6, Issue 2. – P. 41–57.

[24]. Lakhno V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering [Text] / V. Lakhno // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 2, No 9(80): Information and controlling system. – P. 18–25. DOI: 10.15587/1729-4061.2016.66015.

REFERENCES

[1]. Abidar, R., Moummadi, K., Moutaouakkil, F., Medromi, H. (2015). Intelligent and Pervasive Supervising Platform for Information System Security Based on Multi-Agent Systems. International review on computers and software, Vol. 10, pp. 44–51. doi: 10.15866/irecos.v10i1.4699.

[2]. Alcaraz, C., Zeadally, S. (2013). Critical Control System Protection in the 21st Century. Computer, Vol. 46, pp. 74–83. doi: 10.1109/MC.2013.69.

[3]. Jegede, A. J., Aimufua, G. I. O., Salami, H. O. (2007). Information Security Policy: Relevance, Creation and Enforcement. International Journal of Soft Computing, Vol. 2, pp. 408–410. doi: 10.3923/ijscomp.2007.408.410.

[4]. Ameziane El Hassani, A., Abou El Kalam, A., Bouhoula, A., Abassi, R., Ait Ouahman, A. (2014). Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity. International Journal of Information Security, Vol. 14, No 4, pp. 367–385. doi: 10.1007/s10207-014-0254-9.

[5]. 2015 Cyber Attacks Statistics (2016). Available at: http://www.hackmageddon.com /2016/ 01/ 11/ 2015 - cyber-attacks-statistics.

[6]. Dudykevych, V. B., Prokopyshyn, I. A., Chekurin, V. F. (2012). The problems of assessing the effectiveness of protection systems., Bulletin of Nacional University "Lviv Politechnic", Automatics of measuremen and control, No 741, pp. 118–122.

[7]. Ghryshhuk, R. V. (2011). Attacks on information in the information and communication systems, Modern special equipment, No 1 (24), pp. 61–66.

[8]. Korchenko, A. A. (2013). The system of formation of fuzzy standards of network parameters, Data protection, No15 (3), pp. 240–246.

[9]. Lahno, V. (2014). Ensuring of information processes' reliability and security in critical application data processing systems. MEST Journal, Vol. 2, pp. 71–79. doi: 10.12709/mest.02.02.01.07.

[10]. Manap, N., Basir, S., Hussein, S., Tehrani, P., Rouhani, A. (2013). Legal Issues of Data Protection in Cloud Computing. International Journal of Soft Computing, Vol. 8, pp. 371–376. doi: 10.3923/ijscomp.2013.371.376.

[11]. George, J. A., Hemalatha, M. (2015). Improving Authentication and Authorization for Identity Based Cloud Environment Using OAUTH with Fuzzy Based Blowfish Algorithm. International review on computers and software, Vol. 10, pp. 783-788. doi: 10.15866/irecos.v10i7.7062.

[12]. Li, H.-H., Wu, C.-L. (2013). Study of Network Access Control System Featuring Collaboratively Interacting Network Security Components. International review on computers and software, Vol. 8, No 2, pp. 527–532.

[13]. Kim, G. Kim, S. (2015). Applying Need Pull and Technology Push Theory to Organizational Information Security Management. International Business Management, Vol. 9, pp. 524–531. doi: 10.3923/ibm.2015.524.531.

[14]. Geetha, R., Kannan, E. (2015). Secure Communication Against Framing Attack in Wireless Sensor Network. International Review on Computers and Software, Vol. 10, No 4, pp. 393-398. doi: 10.15866/irecos.v10i4.5520.

[15]. Shamshirband, S., Anuar, N. B., Kiah, M. L. M., Patel, A. (2013). An appraisal and design of a multiagent system based cooperative wireless intrusion detection computational intelligence technique. Engineering Applications of Artificial Intelligence, Vol. 26, pp. 2105–2127. doi: 10.1016/j.engappai. 2013.04.010.

[16]. Miroshnik, M. A. (2015). Development of methods for evaluating the effectiveness of information security in distributed computer systems, Railway information management systems: scientific journal, No 4 (113), pp. 39–43.

[17]. Lee, K., Kim, J., Kwon, K. H., Han, Y., Kim, S. (2008). DDoS attack detection method using cluster analysis. Expert Systems with Applications, Vol. 34, No 3, pp. 1659–1665. doi: 10.1016/j.eswa. 2007.01.040.

[18]. Dilek, S., Cakır, H., Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, Vol. 6, pp. 21–39. doi: 10.5121/ijaia.2015.6102/

[19]. Patel, A., Taghavi, M., Bakhtiyari, K., Celestino Júnior, J. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications, Vol. 36, pp. 25–41. doi: 10. 1016 / j.jnca.2012.08.007.

[20]. Barman, D. K., Khataniar, G. (2012). Design of Intrusion Detection System Based On Artificial Neural Network and Application of Rough Set. International Journal of Computer Science and Communication Networks, Vol. 2, pp. 548-552. ISSN: 2249–5789.

[21]. Raiyn, J. (2014). A survey of Cyber Attack Detection Strategies. International Journal of Security and Its Applications, Vol. 8, pp. 247–256. doi: 10.14257/ijsia.2014.8.1.23.

[22]. Mukkamala S., Sung A.H., Abraham A., Ramos V. (2006). Intrusion detection systems using adaptive regression splines. Sixth International Conference on Enterprise Information Systems, Part 3, P. 211–218. DOI:10.1007/1-4020-3675-2_25.

[23]. Kotenko, I., Fedorchenko, A., Chechulin, A. (2015). Integrated repository of security information for network security evaluation. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 6, No 2, pp. 41–57.

[24]. Lakhno V. (2016). Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering, Eastern-European Journal of Enterprise Technologies, Vol. 2, No 9(80): Information and controlling system, P. 18–25. DOI: 10.15587/1729-4061.2016.66015.

ВДОСКОНАЛЕННЯ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА РАХУНОК АДАПТИВНИХ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ КІБЕРАТАК

Останні десятиліття ознаменувалися стрімким розвитком критично важливих інформаційних систем (КВІС), для кіберзахисту яких використовують технології виявлення і розпізнавання кібератак. В умовах зростання кількості дестабілізуючих впливів на стан

кібербезпеки КВІС необхідно проводити дослідження, спрямовані на розвиток методологічних і теоретичних основ інформаційного синтезу систем кіберзахисту, здатних до самонавчання.
Показано, що процес кіберзахисту для КВІС контролюється та аналізується за значеннями декількох параметрів ознак аномалій або кібератак. Це, у свою чергу, дає можливість виконувати попередню оцінку інформаційної безпеки КВІС за допомогою методології обробки статистичних даних з виявлених аномалій та кібератак із застосуванням адаптивних сплайнів та подальшої кластеризації набору ознак аномалій або спроб кібернападів. Запропоновано модель побудови адаптивної системи інтелектуального розпізнавання кіберзагроз (АСР). За допомогою двоетапного навчання із застосуванням адаптивних сплайнів та процедури нечіткої кластеризації розроблено алгоритм навчання АСР з можливістю гіперелліпсоїдної корекції вирішальних правил. Це дозволяє створювати адаптивні механізми самонавчання АСР. Перевірена ефективність алгоритму інформаційно-екстремального навчання АСР. Для оцінки якості розбиття простору ознак аномалій, уразливостей та кібератак здійснено вибір раціональної кількості кластерів та показника нечіткості кластерів в просторі ознак. Доведено, що запропонований підхід дає змогу розв'язувати складні задачі управління процесом кіберзахисту КВІС від атак, а також може бути застосований при розробці програмних рішень для систем кіберзахисту.
Ключові слова: критично важливі інформаційні системи, кібербезпека, захист інформації, розпізнавання загроз, аномалії, кластеризація ознак, адаптивні сплайни, інформаційно-екстремальний алгоритм.

IMPROVEMENT OF CYBER DEFFENCE INFORMATION SYSTEMS BY ADAPTIVE TECHNOLOGIES RECOGNITION OF CYBERATTACKS

The last decade showed the rapid development of major-critical information systems (MCIS), where cyber technology detection and identification of cyber-attacks are used for cyber defense. Necessity of further research in the development of methodological and theoretical foundations of information synthesis of self-learning cyber defense systems are caused by growing number destabilizing factors of cyber security of MCIS. This paper contains tasks of improving the stability of MCIS in terms of introduction of new systems and modernization of existing information and automated control systems with increasing number of destabilizing effects on the availability, confidentiality and integrity of information.
The process of cyber defense of MCIS is monitored and analyzed by values of several parameters of abnormalities signs or cyber-attacks. This is make it possible to carry out a preliminary assessment of information security via the clustering feature set of abnormalities or attempted cyber-attacks. Offered a categorical model of development adaptive systems of an intellectual detection of cyber threats (ASIDCT). Algorism of self-learning of ASIDCT is developed with the help of procedure of fuzzy clustering. This allows to create an adaptive self-learning mechanisms of ASIDCT. To assess the quality partitioning area of abnormalities signs, vulnerabilities and cyber-attacks is made a rational set of number of clusters and fuzziness index clusters in features area. It is proved that the offered approach gives the possibility to solve complex problems in control of cyber-attack process of MCIS and can be used in the development of software solutions for cyber defense systems.
Keywords: major-critical information systems, cyber security, information security, threats detection, abnormalities, clustering features, information and extreme algorithm.

Лахно Валерий Анатольевич, доктор технических наук, доцент, заведующий кафедры организации комплексной защиты информации Европейского университета.
E-mail: valss21@ukr.net.
Лахно Валерій Анатолійович, доктор технічних наук, доцент, завідувач кафедри організації комплексного захисту інформації Європейського університету.
Lakhno Valery, Doctor of Science, associate professor, Head of Complex Information Security Organization Department, European University.

Терещук Анна Михайловна, старший преподаватель кафедры информационных систем и математических дисциплин Европейського университета.
E-mail: ganna.tereschuk@gmail.com
Терещук Ганна Михайлівна, старший викладач кафедри інформаційних систем і математичних дисциплін Європейського університету.
Tereshchuk Ganna, Senior lecturer of Department of Information Systems and Mathematical Disciplines, European University.

Петренко Тарас Анатолиевич, старший преподаватель кафедры математического моделирования и кибербезпасности Черниговского национального технологического университета
E-mail: mail_taras@ukr.net
Петренко Тарас Анатолійович, старший викладач кафедри математичного моделювання та кібербезпеки Чернігівського національного технологічного університету
Petrenko Taras, senior lecturer of mathematical simulation and cybersecurity department, Chernihiv National University of Technology (Chernihiv, Ukraine)