КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.23.12215

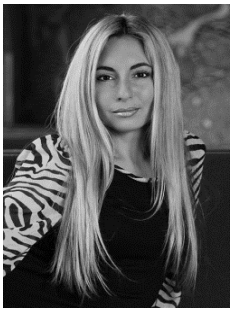
СИСТЕМА ВЫЯВЛЕНИЯ КИБЕРАТАК

Игорь Терейковский[1], Анна Корченко[2]

[1]Национальный технический университет Украины «КПИ им. Игоря Сикорского»
[2]Национальный авиационный университет, Украина

ТЕРЕЙКОВСКИЙ Игорь Анатольевич, д.т.н.

Год и место рождения: 1967 год, г. Тернополь, Украина.
Образование: Киевский институт инженеров гражданской авиации, 1992 год.
Должность: профессор кафедры системного программирования и специализированных компьютерных систем НТУУ "КПИ им.Игоря Сикорского" с 2015 года.
Научные интересы: информационная безопасность.
Публикации: более 100 научных трудов, среди которых монографии, учебные пособия, учебно-методические комплексы дисциплин, научные статьи, материалы и тезисы докладов конференций.
E-mail: terejkowski@ukr.net



КОРЧЕНКО Анна Александровна, к.т.н.

Год и место рождения: 1985 год, г. Киев, Украина.
Образование: Национальный авиационный университет, 2007 год.
Должность: доцент кафедры безопасности информационных технологий.
Научные интересы: информационная безопасность, системы обнаружения вторжений, экспертное оценивание в сфере защиты информации.
Публикации: более 80 научных трудов, среди которых учебные пособия, учебно-методические комплексы дисциплин, научные статьи, материалы и тезисы докладов конференций.
E-mail: annakor@ukr.net

Аннотация. *На сегодня одним из условий обеспечения кибербезопасности в крупных организациях, является непрерывность обеспечения процесса обнаружения вторжений (кибератак). К таким, наиболее распространённым системам, относятся те, которые используют известные сигнатуры (шаблоны) атак в сетевом трафике, а также системы, ориентированные на обнаружение аномалий, содержащие профиль нормальной (ненормальной) активности. Они имеют ряд недостатков, которые перекрывают экспертные подходы, основанные на использовании знаний и опыта специалистов соответствующей предметной области. Расширение воздействий кибератак, направленных на различные ресурсы информационных систем инициирует задачи построения технических решений и создание специальных средств, способных оставаться эффективными при появлении новых видов угроз с неустановленными или нечетко определенными параметрами. Известен ряд достаточно эффективных разработок, используемых для решения таких задач выявления кибератак. С этой целью, на базе известной методологии построения систем выявления аномалий, порожденных кибератаками разработана система выявления атак. Она, за счет баз данных кибератак, правил и эталонов, а также модулей формирования текущих значений, α-уровневой номинализации, идентифицирующих термов, уровня аномальности и визуализации, позволяет строить средства, расширяющие функциональные возможности современных систем обнаружения вторжений. Это достигается посредством определения уровня аномального состояния, характерного воздействию определенного типа кибератак в слабоформализованной нечеткой среде окружения.*

Ключевые слова: *атаки, кибератаки, аномалии, выявление кибератак, выявление аномалий, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, системы обнаружения кибератак.*

Введение

Сегодня системы обнаружения и предотвращения вторжений являются неотъемлемым элементом защиты от различных типов кибератак для каждой серьезной организации. Процесс обнаружения вторжений, это прежде всего активный процесс, который должен находится в непрерывном состоянии и свидетельствовать о попытках несанкционированного вмешательства. В идеальном случае указанные системы предупреждают о подозрительной активности в сети или проникновении, а основное их назначение направлено на выявление фактов несанкционированного доступа в сеть и принятие соответствующих мер противодействия.

Большинство систем обнаружения вторжений (СОВ) дорогостоящие, имеют закрытый код и требуют квалифицированной настройки под конкретные требования организации и сервисы, которую могут осуществлять только специалисты соответствующей предметной отрасли.

Наиболее распространёнными СОВ являются те, которые работают по существующим сигнатурам реализуя поиск шаблонов известных атак в сетевом трафике или высокоуровневых данных. Сигнатурный подход основывается на описании атаки в виде шаблона и его поиска в контролируемом пространстве (например, в протоколах, журнале регистрации и др.). Эта технология достаточно проста, однако существует проблема создания эффективного механизма описания сигнатур, а также фиксации всех возможных модификаций атак.

Также очень востребованы и необходимы СОВ, которые ориентированы на обнаружение аномальных состояний. Они, как правило, содержат профиль нормальной (ненормальной) активности системы и детектируют отклонения от него. Эти СОВ основываются на гипотезе, что аномальное состояние проявляется как отклонение от нормального, но аномальное не всегда порождается атакой или ее частью. Чаще всего для обнаружения аномалий используется аппарат математической статистики, нейронные сети, марковские модели, вейвлет анализ, искусственные иммунные системы, иммунокомпьютинг и др. Недостатками аномальных СОВ являются: высокий уровень ложных срабатываний, поскольку любое (даже не опасное) отклонение от нормальной активности спровоцирует реакцию системы; сложность создания обучающей выборки; сложность внедрения и настройки, поскольку стратегия обучения и характер данных для обучающей выборки зависит от специфики вычислительной среды.

Существенный недостаток современных аномальных СОВ также связан с длительностью процесса создания соответствующего профиля нормального состояния системы, а при ее реконфигурации, модификации и других изменениях набранная статистика становится неактуальной или неполной. Следует также отметить, что вся статистика о системе будет тогда, когда она прекратит свое существование в том виде, в котором она исследовалась, но потребность в ней уже будет отсутствовать.

Более эффективные в этом отношении являются экспертные подходы, основанные на использовании знаний и опыта специалистов соответствующей предметной области [1].

Исходя из этого построение технических решений и создание средств (систем обнаружения вторжений, выявления кибератак и др.), позволяющих детектировать ранее неизвестные кибератаки (в том числе и 0-day атаки), например, путем контроля текущего состояния нечетко определенных параметров слабоформализованной среды окружения, основанного на экспертных подходах, является актуальной научной задачей.

На базе методологии построения систем выявления аномалий, порожденных кибератаками [2], в основу которой заложен логико-лингвистический подход [1] и кортежная модель [3, 4], а также разработанных методах: формирования лингвистических эталонов [5-8]; фаззификации параметров на лингвистических эталонах [9]; α-уровневой номинализации нечетких чисел [10]; определения идентифицирующих термов [11]; формирования базовых детекционных правил [12], построим систему выявления кибератак (СВК). Она позволит эффективно детектировать в слабоформализованной нечетко определенной среде аномальное состояние за заданный временной промежуток.

Структурное решение СВК отображено на рис. 1. Оно содержит согласованные по параметрам базы данных кибератак (БДК), правил (БДП) и эталонов (БДЭ), а также модули формирования текущих значений (МФТЗ), α-уровневой номинализации (МАУН), идентифицирующих термов (МИТ), уровня аномальности (МУА) и визуализации (МВ).

База БДК содержит множество идентификаторов (ИД) кибератак CA_i $(i=\overline{1,n})$ (см. (1) в [3]), посредством которых осуществляется однозначное определение атаки в процессе присвоения ее имени конкретному ИД (см. этап 1 в [2]).

База БДП состоит из бинарных решающих функций SF_{ia} $(i=\overline{1,n},\ a=\overline{1,w_i})$ (см. (15) в [12]) и идентификаторов аномальности IA_{iu} $(i=\overline{1,n},\ u=\overline{1,v_i})$ (см. (5) в [12]), входящих в множества базовых правил $\mathbf{DR_i}$ $(i=\overline{1,n})$ (см. (21) в [12]), необходимых для обнаружения i-й кибератаки посредством параметрических подсред различной размерности (см. этап 7 в [2]).

База БДЭ содержит множество лингвистических эталонов $\underset{\sim}{T}^{e}_{ijs}$ $(i=\overline{1,n},\ j=\overline{1,m_i},\ s=\overline{1,r_j})$ (см. (29) в [5]), предназначенных для отображения состояния множеств соответствующих параметров $\mathbf{P_i}$ $(i=\overline{1,n})$ в определенной среде окружения, направленных на выявление кибератаки с ИД CA_i (см. этап 3 в [2]).

Модуль МФТЗ предназначен для формирования всех возможных текущих значений нечетких параметров $\underset{\sim}{P}^{tf}_{ij}$ $(i=\overline{1,n},\ j=\overline{1,m_i})$ (см. этап 2 в [2]), получаемых посредством $\mathbf{T^e_i}$ $(i=\overline{1,n})$ в опре-

деленный момент времени τ_f за заданный промежуток, длительность которого $\tau_h = \tau_f - \tau_{f-1}$ ($f = \overline{1,max_\tau}$) [3].

Модуль МАУН осуществляет эквивалентные преобразования нечетких чисел (НЧ) посредством приведения всех эталонных $\tilde{T}^{e}_{ijs}$ и текущих $\tilde{P}^{\tau_f}_{ij}$ ($i = \overline{1,n}$, $j = \overline{1,m_i}$, $s = \overline{1,r_j}$) к номинальному (одному для всех) числу компонент на основе подмножеств α-уровневых интервалов $\mathbf{AL^{Ie}_{ij}}$ и межточечных α-уровневых интервалов $\mathbf{AL^{Ip}_{ij}}$ (см. этап 5 в [2]) [10].

Модуль МИТ ориентирован на поиск, по заданной лингвистической переменной, идентифицирующего эталонного терма (т.е. его номера, а $s = NUM_{ij}$), по которому с помощью детекционных правил можно определить уровень аномального состояния, характерного для определенного типа кибератак (см. этап 6 в [2]) [11].

Модуль МУА необходим для формирования $DR_{iw_i s}$ на основе идентифицирующего эталонного терма (использование NUM_{ij}), эталонного преобразованного НЧ $\tilde{T}^{ep}_{ijs}$, а также идентификаторов аномальности IA_{iu} и бинарных решающих функций SF_{ia}, посредством обработки подмножеств условных детекционных выражений $\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i}\{\bigcup_{u=1}^{v_i} if\ SF_{ia}\ then\ IA_{iu}\}\}$ ($i = \overline{1,n}$, $a = \overline{1,w_i}$, $u = \overline{1,v_i}$), которые отображают формируемые базовые правила для обнаружения i-й кибератаки с использованием параметрических подсред различной размерности (см. этап 7 в [2]) [12].

Модуль МВ используется для графической интерпретации полипараметрической мультиразмерной среды [2], распределения идентификаторов атакующих действий и фаззифицированных значений текущих параметров $\tilde{P}^{\tau_f p}_{ij}$ относительно лингвистических эталонов $\mathbf{T^{ep}_{ij}}$ в виде выявленной области, характеризующей атаки, а также отображения условного выражения ($DR_{iw_i s}$) базового детекционного правила, согласно которому было осуществлено выявление кибератак.

Система СВК (построение которой осуществляется согласно известной методологии [2] посредством 7 этапов) согласно алгоритму, представленному на рис. 1, функционирует следующим образом.

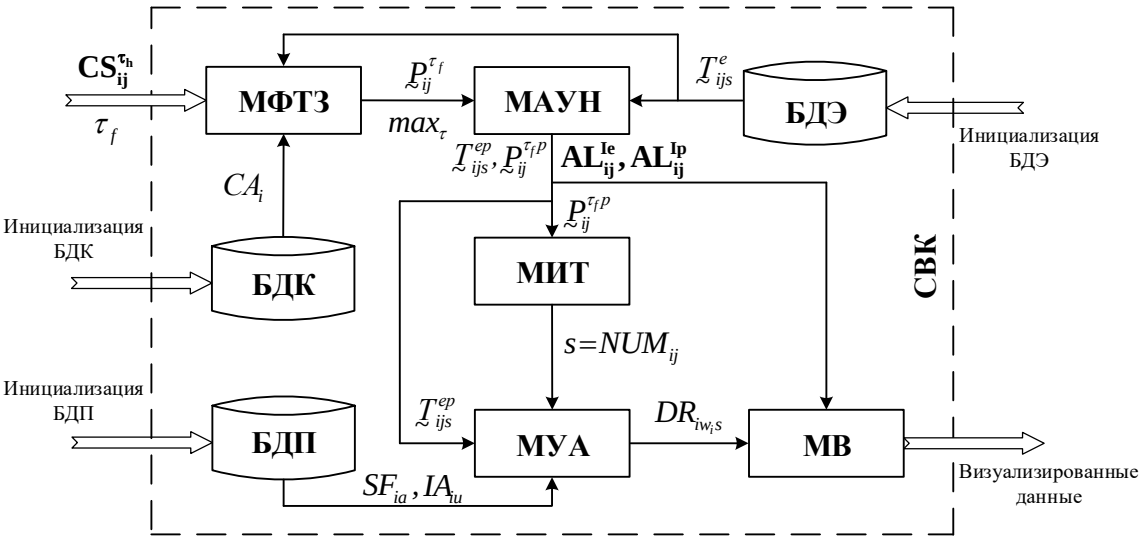


Рис. 1. Структурная схема СВК

Условно работу СВК можно представить двумя процессами: 1) процесс инициализации БД; 2) процесс выявления кибератак (см. рис. 2).

Процесс инициализации БД связан с наполнением (модификацией) БДК, БДП и БДЭ (см. соответственно вершины 1-3, 8; 1, 2-8; и 1, 2, 9-12 на рис. 2). При необходимости, на этапе функционирования СВК, указанные БД могут подвергаться модификации.

Процесс выявления кибератак CA_i осуществляется за заданный временной промежуток τ_h в каждый момент времени τ_f ($f = \overline{1,max_\tau}$, где max_τ – максимальный номер временного промежутка f) (см. вершину 13 на рис. 2) на основе множества значений счетчиков сенсоров $\mathbf{CS_{ij}}$ (см. (3) в [9] и вершины 14-16), показатели которых зависят от τ_h ($\mathbf{CS^{\tau_h}_{ij}}$), а аткже эталонных НЧ $\tilde{T}^{e}_{ijs}$, которые передаются из БДЭ и поступают в модуль МФТЗ, где формируются текущие значения нечетких параметров $\tilde{P}^{\tau_f}_{ij}$ и определяется max_τ (см. вершины 17-20).

Далее с БДЭ и МФТЗ соответственно эталонные $\tilde{T}^{e}_{ijs}$ и текущих $\tilde{P}^{\tau_f}_{ij}$ НЧ поступают в МАУН, где осуществляется их α-уровневая номинализация (см. рис. 2 вершины 21-24).

В результате этого с МАУН на вход МИТ поступают преобразованные НЧ $\tilde{T}^{ep}_{ijs}$ и $\tilde{P}^{\tau_f p}_{ij}$, где определяются идентифицирующие термы (у кото-

рых $s = NUM_{ij}$), отображающие аномальность текущего состояния среды окружения, порожденную определенными кибератаками (см. вершину 25 на рис. 2). Далее, на основе полученных в МАУН идентифицирующих термов $\underset{\sim}{T}^{ep}_{ijs}$ и термов, для которых $s = NUM_{ij}$, поступивших с МИТ, а также бинарных решающих функций SF_{ia} (см. (15) в [12]) и идентификаторов аномальности IA_{iu} (см. (5) в [12]), поступающих с БДП, в МУА формируются подмножества базовых правил $\mathbf{DR_i}$ (см. (21) в [12]), посредством которых определяется условное выражение $DR_{iw_i s}$, по которому осуществляется выявление i -й кибератаки (см. вершину 26 на рис. 2).

На основании подмножества α-уровневых интервалов $\mathbf{AL^{Ie}_{ij}}$, межточечных α-уровневых интервалов $\mathbf{AL^{Ip}_{ij}}$, а также всех преобразованных $\underset{\sim}{T}^{ep}_{ijs}$ и $\underset{\sim}{P}^{\tau_f p}_{ij}$, поступивших с МАУН и условного выражения $DR_{iw_i s}$, поступившего с МУА, в МВ графически интерпретируются идентификаторы атакующих действий (отображаемые посредством многомерных (например, двумерных или трехмерных) опорных областей, например, Н, БНВ, ББН, В, П [13]) и фаззифицированные значения текущих параметров $\underset{\sim}{P}^{\tau_f p}_{ij}$ относительно лингвистических эталонов $\mathbf{T^{ep}_{ij}}$ соответственно (см. вершину 27 на рис. 2).

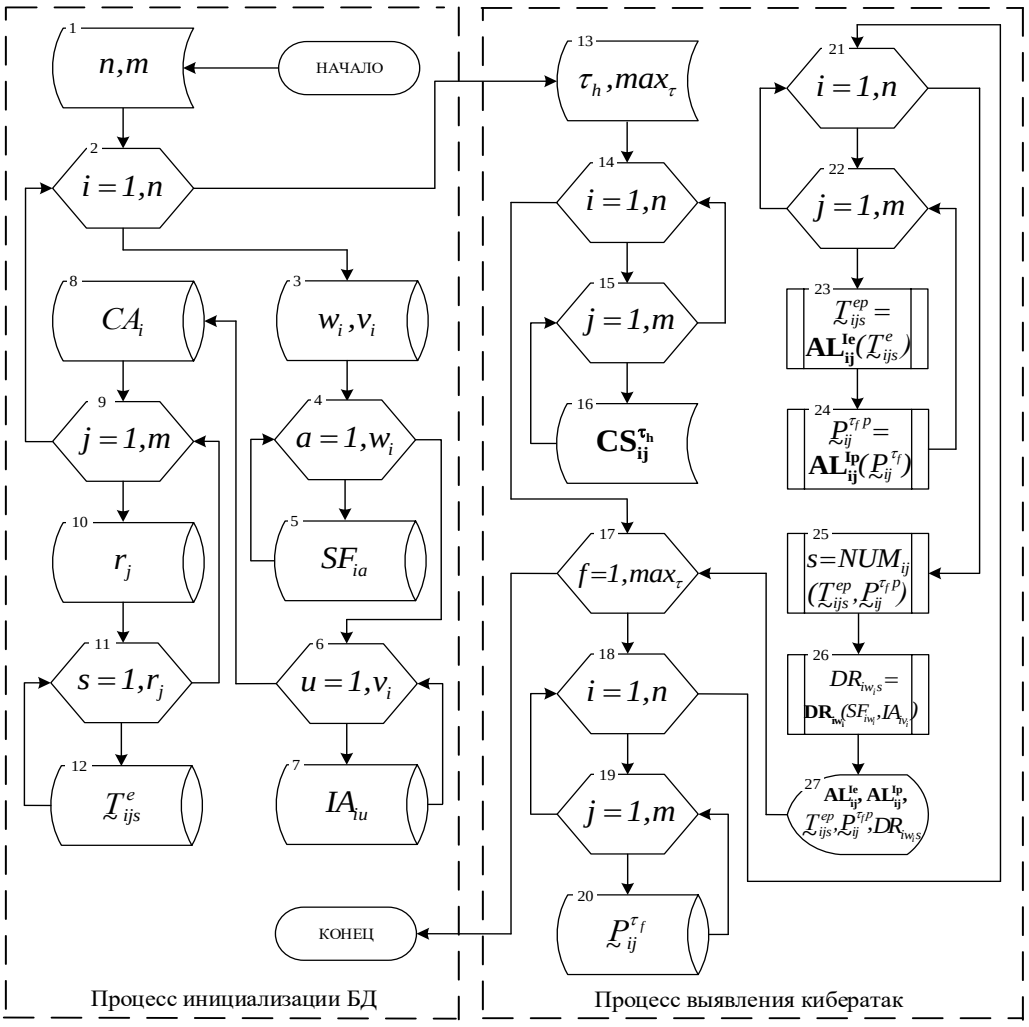


Рис. 2. Алгоритм работы СВК

Выводы

Таким образом, в работе предложена СВК, которая за счет баз данных кибератак, правил и эталонов, а также модулей формирования текущих значений, α-уровневой номинализации, идентифицирующих термов, уровня аномальности и визуализации позволяет строить средства, расширяющие функциональные возможности современных СОВ, посредством определения уровня аномального состояния, характерного воздействию определенного типа кибератак в слабоформализованной нечеткой среде окружения.

Литература

[1] А. Корченко, «Построение систем защиты информации на нечетких множествах», Теория и практические решения, К.:МК-Пресс, 320 с., 2006.

[2] А. Корченко, В. Щербина, Н. Вишневская, «Методология построения систем выявления аномалий порожденных кибератаками», *Захист інформації*, №1, Т.18, с. 30-38, 2016.

[3] А. Корченко, «Кортежная модель формирования набора базовых компонент для выявления кибератак», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В.2 (28), с. 29-36, 2014.

[4] A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», *Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015)*, Warsaw, Poland, September 24-26,: Vol. 1, pp. 478-483, 2015.

[5] А. Корченко, «Метод формирования лингвистических эталонов для систем выявления вторжений» *Захист інформації*, Т.16, №1, с. 5-12, 2014.

[6] И. Терейковский, А. Корченко, П. Викулов, А. Шаховал, «Модели эталонов лингвистических переменных для обнаружения сниффинг-атак», *Захист інформації*, №3, Т.19, с. 228-242, 2017.

[7] B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, «Improved method for the formation of linguistic standards for of intrusion detection systems», *Journal of Theoretical and Applied Information Technology*, vol.87. №.2, p. 221-232, 2016

[8] M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, «The Etalon Models of Linguistic Variables for Sniffing-Attack Detection», *Proceedings of the 2017 IEEE 9th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2017)*, Romania, Bucharest, September 21-23, Vol. 1, p. 258-264, 2017:

[9] А. Корченко, «Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак», *Безпека інформації*, № 1 (20), с. 21-28, 2014.

[10] А. Корченко, «Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений», *Захист інформації*, Т.16, №4, с.292-304, 2014.

[11] А. Корченко, «Метод определения идентифицирующих термов для систем обнаружения вторжений», *Безпека інформації*, Т.20, № 3, с. 217-223, 2014

[12] Н. Карпинский, А. Корченко, С. Ахметова, «Метод формирования базовых детекционных правил для систем обнаружения вторжений», *Захист інформації*, №4, Т.17, с. 312-324, 2015.

[13] A. Korchenko, Z. Alimseitova, N. Zhumangaliyeva, «A system for identifying anomaly state in informational systems», *VII Inter University Conference of Students, PhD Students and Young Scientists «Engineer of XXI Century»*, Poland, Vol.2, p. 39-48, 2017.

УДК 004.056.53(045)

Терейковський І.А., Корченко А.О. Система виявлення кібератак

Анотація. *На сьогодні однією з умов забезпечення кібербезпеки в великих організаціях, є безперервність забезпечення процесу виявлення вторгнень (кібератак). До таких, найбільш поширених систем, відносяться ті, які використовують відомі сигнатури (шаблони) атак в мережевому трафіку, а також системи, орієнтовані на виявлення аномалій, що містять профіль нормальної (ненормальною) активності. Вони мають ряд недоліків, які перекривають експертні підходи, засновані на використанні знань і досвіду фахівців відповідної предметної області. Розширення впливів кібератак, спрямованих на різні ресурси інформаційних систем, ініціює завдання побудови технічних рішень і створення спеціальних засобів, здатних залишатися ефективними при появі нових видів загроз з невстановленими або нечітко визначеними параметрами. Відомий ряд досить ефективних розробок, який використовуються для вирішення таких завдань виявлення кібератак. З цією метою, на базі відомої методології побудови систем виявлення аномалій, породжених кібератаками розроблена система виявлення атак. Вона, за рахунок баз даних кібератак, правил і еталонів, а також модулів формування поточних значень, α-рівневої номіналізації, ідентифікуючих термів, рівня аномальності і візуалізації, дозволяє будувати засоби, що розширюють функціональні можливості сучасних систем виявлення вторгнень. Це досягається за допомогою визначення рівня аномального стану, характерного впливу певного типу кібератак в слабоформалізованому нечіткому середовищі оточення.*

Ключові слова: *атаки, кібератаки, аномалії, виявлення кібератак, виявлення аномалій, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, системи виявлення кібератак.*

Tereykovsky I., Korchenko A. Cyberattack detection system

Abstract. *Today, one of the conditions for providing cybersecurity in large organizations is ensure the continuity of the intrusion detection (cyberattack) process (cyberattacks). The most common are systems, which using known attacks signature (patterns) in network traffic and the systems, which oriented at detecting abnormalities that contain the normal (abnormal) activity profile. That systems have a number of disadvantages that overlap expert approaches based on the use of knowledge and experience of specialists in the relevant subject area. Extending the influence of cyberattacks, oriented to various information systems resources, initiates the task of constructing technical solutions and developing special tools that can remain effective when new types of threats appear with unidentified or unclear parameters. There are a number of very effective developments, which are used to solve such tasks of detecting cyberattacks. For this purpose, based on the well-known methodology for building of detecting anomalies systems, generated by cyberattacks, attacks detecting system was developed. The developed system, at the expense of cyberattacks databases, rules and standards, modules for the formation of current values, α-level denomination, identifying terms, level of abnormality and visualization, allows to build tools that expand the functional capabilities of modern systems of intrusion detection. This is achieved by determining the level of the abnormal state, the characteristic effect of a certain type of cyberattack in faintly formalized fuzzy environment.*

Key words: *attacks, cyberattacks, anomalies, detection of cyberattacks, detection of anomalies, intrusion detection systems, anomaly detection systems, attack detection systems, cyberattack detection systems.*

Отримано 16 *жовтня 2017 року*, затверджено редколегією *30 жовтня 2017 року*