КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.169183
УДК 004.056 004.056.53

**Толюпа Сергій Васильович**
доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-1919-9174
*tolupa@i.ua*

**Плющ Олександр Григорович**
кандидат технічних наук, доцент, професор кафедри Мобільних та відеоінформаційних технологій
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0001-5310-0660
*opliusch@yahoo.com*

**Пархоменко Іван Іванович**
кандидат технічних наук, доцент, доцент кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0001-6889-9284
*parkh08@ukr.net*

# ПОБУДОВА СИСТЕМ ВИЯВЛЕННЯ АТАК В ІНФОРМАЦІЙНИХ МЕРЕЖАХ НА НЕЙРОМЕРЕЖЕВИХ СТРУКТУРАХ

**Анотація.** Системи виявлення мережевих вторгнень і виявлення ознак атак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем. На сьогодні системи виявлення вторгнень і атак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій.

У статті запропоновано програмний прототип системи виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних та нейромережевих структур. Проведені експериментальні дослідження підтверджують ефективність створеної моделі виявлення для захисту інформаційної мережі. Проведені експерименти з програмним прототипом показали високу якість виявлення мережевих атак на основі нейромережевих структур та методів інтелектуального розподілу даних. Проаналізовано стан захищеності інформаційних систем по протидії від кібератак, що дало можливість зробити висновки, що для забезпечення безпеки кіберпростору необхідне впровадження комплексу систем і механізмів захисту, а саме систем: розмежування доступу користувачів; міжмережного екранування; криптографічного захисту інформації; віртуальні приватні мережі; антивірусного захисту елементів ІТС; виявлення і запобігання вторгнень; автентифікації, авторизації і аудиту; попередження втрати даних; управління безпекою та подіями; управління захищеності.

**Ключові слова**: кіберпростір, атака, нейромережа, інформаційна мережа, системи виявлення атак, методи інтелектуального аналізу даних, тренувальна база, нечітка логіка, каутеризація, кіберзахист.

## 1. ВСТУП.

Безпечне існування громадянського суспільства і держави безпосередньо залежить від діяльності та умов функціонування об’єктів її інфраструктури, а також

різноманітних систем та мереж, що складають інформаційно-комунікаційне середовище. Вагома частина систем, об'єктів і ресурсів складають таку важливу для функціонування економіки, суспільства і держави нішу, що навіть, здавалося, незначне їх пошкодження може призвести до негативних наслідків на загальнонаціональному рівні. Перераховане вище відносять до критичної інфраструктури, і саме їх захист має бути першочерговим завданням державного управління для сучасної країни.

**Постановка проблеми.** У 2020 році в Україні зафіксували близько одного мільйона випадків кіберзагроз. Серед них - мережеві атаки, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення. З метою попередження можливих атак, Національний координаційний центр кібербезпеки (НКЦК) посилив співпрацю з приватними компаніями. Вони передбачають обмін інформацією про кіберзагрози та інциденти в сфері кіберзахисту для оперативного інформування, реагування, попередження можливих атак і взаємодопомоги [1].

При цьому особливу занепокоєність викликає можливість застосування інформаційних технологій у кібернетичному просторі в інтересах здійснення військово-політичного та силового протиборства, тероризму та проведення хакерських атак. Експерти передбачають, що в прийдешньому році повністю зміниться структура кібероперацій і те, як вони проводяться. Вони стануть більш непомітними для систем виявлення і фаєрволом. Аналіз робіт, що ведуться в даній області, показує, що зазначена проблема потребує подальшого вивчення як з точки зору побудови адекватних математичних моделей предметної області, так і реалізації ефективних алгоритмів виявлення атак і прийняття рішень, що підтверджує актуальність досліджень в даній предметній області.

**Відомі підходи до вирішення поставленої задачі.** На сьогоднішній день існує велика кількість різноманітних методів та засобів захисту від кібератак на об'єктах інформаційної діяльності. Нажаль на теперішній час не існує абсолютно універсального методу протидії кібератакам і тому виникає необхідність комплексного підходу до вирішення даної задачі. Застосування методів інтелектуального аналізу даних та штучного інтелекту дає можливість підвищити ефективність протидії вторгненням і захистити об'єкти від потенційних порушників. Ряд сучасних систем виявлення вторгнень використовують різні методи інтелектуального аналізу даних для виявлення атак і вторгнень. В основі таких систем лежать різні методики: методи Data Mining; пошук асоціативних правил; побудова імунних систем; марковскі процеси; дерева прийняття рішень; генетичні алгоритми; нейронні мережі.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії кібератакам. Для виявлення мережевих вторгнень використовуються сучасні методи [2-5], моделі [6, 7], засоби [8-10], програмне забезпечення [11] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [12-14], які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями,

зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому, системи виявлення вторгнень (СВВ) повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

На сьогодні вирішення питань забезпечення безпеки в ІС та управління станом їх захищеності описується в роботах вітчизняних та закордонних дослідників, а саме: Бурячка В.Л., Гнатюка С.О., Корченко О.Г., Кузнецова О.О., Субача І.Ю., Євсеєва С.П., Дудикевича В.Б., Казмирчук С.В., T. Ptaceka, G. Elmasry, P. Albers, O. Camp та інших.

Слід зазначити, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в ІС з боку неавторизованої сторони (НАС). Також слід наголосити, що атаки на ІС з кожним роком стають все досконалішими, глобальнішими та частішими.

## 2. МЕТОДИКА ТА РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

При розробці та проведенні досліджень систем виявлення вторгнень однією з ключових завдань є вибір масивів даних, на яких буде проводитися тестування. Великі компанії-розробники в першу чергу орієнтуються на власні бази даних, спеціалізовані під конкретні завдання і область застосування.

Серед лідерів детектування вразливостей можливо зазначити наступних розробників відповідних баз даних вразливостей: компанія MITRE та її база вразливосей Common Vulnerabilities and Exposures (CVE); National Institute of Standardsand Technology та база National Vulnerabilities Database (NVD); United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND), компанія IBM та база вразливостей X-Force та інші.

Питання вибору тренувальної бази з атаками не має простого рішення, тому що широко поширені бази даних містять багато в чому застарілі типи атак, а більш сучасні бази мають специфічну структуру, що вимагає складної попередньої обробки, і використовуються тільки окремими дослідниками, що перешкоджає порівнянні якісних показників результатів роботи. На сьогоднішній день можна виділити дві найбільш поширені тренувальні бази даних з відомими атаками – DARPA [15] і KDD [16].

Тренувальна база даних DARPA (Defense Advanced Research Project Agency) була сформована в рамках дослідження можливостей різних систем виявлення вторгнень. Під час цього дослідження використовувалися дані мережевого трафіку й відомості від файлової системи для можливості ідентифікації змодельованих вторгнень, проведених фахівцями під час запису мережевих дампов. Інформація про атаки DARPA зберігається у вигляді текстового опису, в якому вказується час початку атаки, тривалість, адреса жертви, назва атаки, категорія атаки та інші параметри.

На відміну від тренувальних даних DARPA, база даних KDD (рис. 1) містить не дампи мережевого трафіку, а оброблені відомості у вигляді масивів з 42 ключових значень. Дана база успішно застосовується багатьма дослідниками для аналізу застосовності різних математичних методів в завданню виявлення мережевих атак, в

основному через можливість використання масивів даних з більшості програмних засобів без виконання додаткової обробки [17].

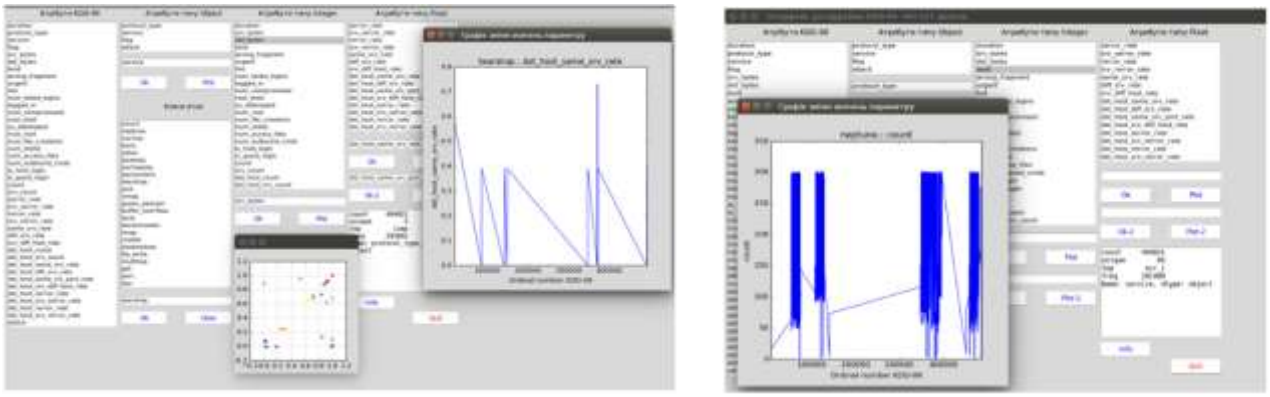

*Рис. 1. Інтерфейс ьренувальної бази KDD*

Системи виявлення мережевих атак збирають інформацію з пакетів мережевого трафіку, системних журналів і показників функціонування системи. Традиційні системи виявлення мережевих атак будуються на сигнатурному підході: за допомогою набору правил або сигнатур, що формуються експертами і розміщені в базу вирішальних правил, описуються всі можливі сценарії і особливості атак. У цього підходу існує безліч відомих недоліків. За допомогою аналізу сигнатур неможливо виявити нові види атак, тому що база вирішальних правил не містить інформації про відповідну атаку. Перераховані проблеми підходу пошуку сигнатур змушують фахівців шукати альтернативні шляхи для організації захисту від мережевих атак. Одним з популярних напрямків досліджень є застосування різних методів інтелектуального аналізу даних (ІАД) в системах виявлення мережевих атак. В основі даних методів лежить припущення, що вся легітимна активність в системі може бути представлена у вигляді математичної моделі. Застосовувані для виявлення мережевих атак методи інтелектуального аналізу даних переслідують одну з наступних цілей: виявлення порушень; виявлення аномалій.

Запропоновані методи включають інтелектуальні властивості штучного інтелекту, а один із цих методів – нейронні мережі. Інтерес до штучних нейронних мереж викликаний тим фактом, що людський мозок виробляє обчислювальні операції принципово іншим чином, ніж звичайна цифрова обчислювальна машина [18]. Нейронні мережі являють безліч інструментів для самих різних застосувань: кластеризація даних, витяг ознак, скорочення розмірності і т.д. В роботі [19] застосовується модифікована версія навчання з підкріпленням для вивчення нових атак. При зустрічі нової атаки використовується зворотний зв'язок для оновлення сигнатур.

У роботах [20, 21] використовуються ієрархії нейронних мереж для виявлення аномалій. Нейронні мережі навчаються з використанням даних, які охоплюють нормальний простір і здатні розпізнавати невідомі атаки. В роботі [21] повідомляється про реальний час рішення для виявлення відомих і невідомих атак за допомогою неконтрольованих нейронних мереж.

У роботі [22] використовуються поворотні багаторівневі персептрони, що класифікують мережеві дані як аномальні і нормальні. Запропонована мережа має можливість кодування тимчасової інформації. Автори розробляють інкрементне ядро

методу головних компонент для попередньої обробки даних, які надходять в нейронну мережу.

В основі більшості СВВ лежить процес класифікації, яка формує висновок про фіксацію атаки або аномальної поведінки. За результатами аналізу безлічі досліджень в якості класифікатора обраний метод опорних векторів [23]. Даний метод показує одні з кращих показників виявлення атак і має широкі можливості по внутрішньому налаштуванню. Метод опорних векторів відшукує зразки, що знаходяться на кордонах між двома класами, які і називаються опорними векторами. Решта функціональні завдання, які вирішуються системами виявлення мережевих атак, в основному спрямовані на підвищення якості виявлення, швидкодії системи, уніфікації і виконання інших допоміжних завдань.

Також нейронні мережі можна використовувати в методах скорочення розмірності - пошук простору меншої розмірності, в якому зберігаються внутрішні властивості вихідних даних. Ці методи дозволяють визначити безліч найбільш важливих параметрів для виявлення конкретної атаки (тренувальна база KDD 42 значення). Вибір конкретного методу скорочення розмірності сильно залежить від тренувальних даних. Для розв'язуваної задачі найбільш перспективними є метод головних компонент [24,25].

Можна вирішувати дану задачу і на основі кластерного аналізу - розбивка безлічі даних на групи таким чином, щоб мінімізувати відмінності між елементами однієї групи і максимізувати відмінності між елементами різних груп. Основні методи кластерного аналізу підрозділяються на ієрархічні і неієрархічні. Ієрархічні методи дозволяють побудувати оптимальну структуру кластерів, але мають експонентну залежність від кількості записів. У зв'язку з великими розмірами масивів тренувальних даних застосування ієрархічної кластеризації до всього масиву даних неможливо. Але при розгляді фрагментів тренувальних даних, що містять записи окремих атак, обсяг інформації дозволяє застосувати ієрархічну кластеризацію.

Як показав аналіз застосування кожного з цих методів одноосібно не дасть позитивного ефекту і тому виникає питання комплексного підходу. Де ключове значення приділемо нейромережевим структурам розпізнавання.

Структура інтелектуальної нейромережевої системи (ІНМС) містить *m*-нейронних ансамблів (шарів), які визначаються кількістю кластерів, що розпізнаються. Кластер відповідає нейронному шару, а їх число визначається кількістю типів атак (рис. 2).

Враховуючи те, що кожний тип атаки має свій образ (портрет), то простір кластера породжує нейронний ансамбль статистичним описом кластера через імовірний портрет (імовірну матрицю). Таким чином, кількість шарів у структурі буде визначатися кількістю кластерів.

Число нейроподібних елементів (нейронів) у шарі, визначається обсягом статистичної вибірки (кількість ознак). При цьому великі статистичні вибірки збільшують розмірність кластерів, представлених портретом (набором параметрів), а малі не дозволяють однозначно зв’язати симптоми з діагнозом. Оптимальним буде портрет кластера, що дозволяє одержати необхідний обсяг інформації. При цьому обсяг статистичної вибірки буде визначатися кількістю параметрів, що характеризують даний тип атаки. Таким чином, кількість нейроподібних елементів у нейронному ансамблі буде визначатися портретом кластера й кількістю параметрів атаки. Сукупність нейронних ансамблів (шарів) являє собою нейронну мережу. Такі нейромережі є спрощеною марковською моделлю.

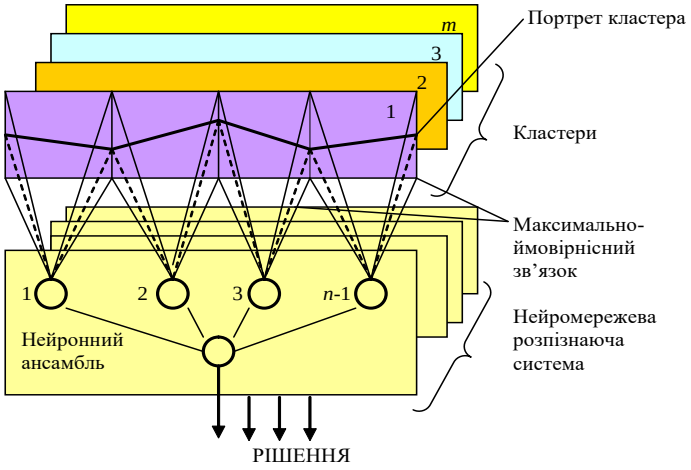


*Рис. 2. Структура інтелектуальної нейромережевої системи розпізнавання*

Сукупність кластерів, які необхідно розпізнати, і впливів, що діють на інформаційну систему (ІС), можуть бути представленні у виді динамічних систем. Ці зміни ідеалізуються як миттєві й називаються подіями та представляються у виді портретів. Під цим терміном, що охоплює відповідні поняття фізичного та інформаційного характеру, розуміється заняття динамічної розподіленої мережі визначеного стану чи конфігурації станів системи. Еволюційні зміни, що проходять між подіями, не приймаються до уваги й вважається, що динаміка системи розвивається дискретно від події до події. Така система є дискретно-подійною.

Дискретно-подійні системи (ДПС) можуть бути представленні тільки стохастичними у виді логічних, алгебраїчних чи орієнтованих на функціонування моделей. Математичний апарат для опису стохастичних моделей, орієнтованих на функціонування ДПС, обраний на основі марковських полів. Таке математичне представлення дозволяє описати функціонування ДПС як елемента зовнішнього середовища і оптимально відобразити його на структуру детермінованої частини нейромережі.

Число станів ДПС визначається точністю кусково-постійної апроксимації неперервної фазової траєкторії динамічного портрета. Підвищення точності кусково-постійної апроксимації фазової траєкторії безперервної системи вимагає введення простору кластерів $A$ великої розмірності, що затрудняє аналітичний опис. Виходом із положення є можливість збільшення (склеювання) станів, тобто перехід від простору конфігурацій $\Omega = \mathrm{A}^T$ до простору станів $\Omega_B = B^T$. Нові макростани можуть бути отримані шляхом об'єднання колишніх станів таким чином:

$$B_к = \sum_{j \in \{K\}} A; k = 1,..., p;\ j = 1,..., r;\ p < r,$$

де $\{K\}$ - множина індексів станів системи $\{A_j\}$ об'єднаних у $B_K$.

Зовнішнє середовище для нейромережевої системи (НМС) може бути представлено у виді сукупності розпізнавання дискретно-подійних систем із зв'язаними дискретними станами.

Узагальнена модель проблено-орієнтованої НМС має структуру (рис. 3), яка включає:

- сенсорну матрицю, що сприймає інформаційне марковське поле у вигляді сукупності спостережень;
- сукупність нейронних ансамблів (класифікаторів), визначається числом кластерів M;
- нейронне поле, що враховує апріорну інформацію у вигляді ймовірностей гіпотез P;
- нейронне поле, що враховує значення елементів платіжної матриці C;
- мажоритарну мережу, що приймає рішення *Г* про розпізнання;
- підсистему (підмережу) навчання.

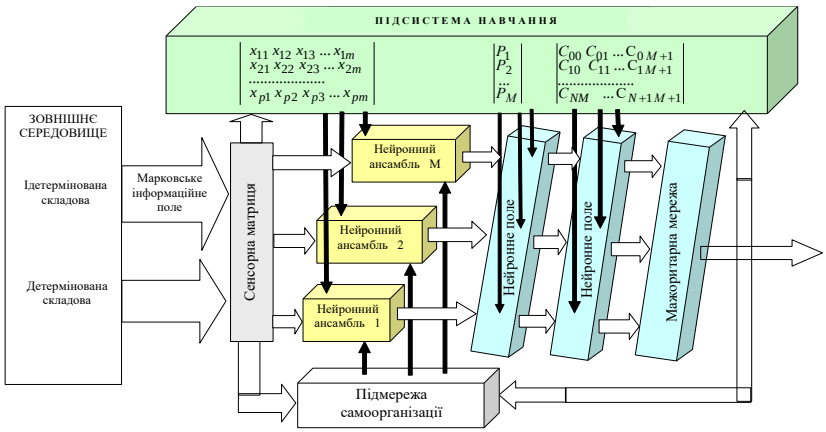


*Рис. 3. Узагальнена модель проблемно-орієнтованої НМС*

Маючи обмежену чисельність вимірів ознак, отриманих з ІС, необхідно розробити таку процедуру обробки параметрів, що дозволяє автоматично одержувати інформацію про стан системи.

Ознаки сприймаються сенсорною матрицею у вигляді сукупності спостережень: $X = (X_1, X_2, ..., X_i, ..., X_m)$, $i$ = 1,2,...,$n$.

В окремому сенсорному каналі відбувається редукція вибіркового простору $X$, у результаті якої маємо послідовність дискретних змінних $U_k$, $k$ = 0,1,...,$n$-1, які приймають значення $Z_1, Z_2,...,Z_r$.

Необхідно синтезувати структуру нейроподібного класифікатора, що реалізує вирішальну функцію $\gamma(U)$ на скороченому вибірковому просторі $U$.

Послідовність дискретних змінних $U_r$, $k$ = 0,1,...,$n$-1, які приймають значення $z_a$, $a$ = 1,2,...,$r$, можна апроксимувати векторами $\Xi$, $\Phi(0)_\mu$ та $\Xi$, $\Phi(k)_\mu$.

Використовуючи векторні позначення, можна записати:

$$ln1_\mu = (\Xi, \Phi(0)_\mu) + (\Xi, \Phi(k)_\mu) = |\Xi||\Phi(0)_\mu| \cos(\Xi \hat{} \Phi(0)_\mu) + |\Xi|, |\Phi(k)_\mu| \cos((\Xi \hat{} \Phi(k)_\mu)),$$

де $|\Xi||\Phi(0)_\mu|, |\Phi(k)_\mu|$ - модулі векторів $\Xi$, $\Phi(0)_\mu$, $\Phi(k)_\mu$;

$(\Xi \hat{} \Phi(0)_\mu)$, $(\Xi \hat{} \Phi(k)_\mu)$ - кути між цими векторами.

Зазначений вище вираз цілком визначає оптимальну структуру класифікатора при фіксованих $j$ та $i$. Він дозволяє виконати інтерпретацію функціонування синтезованої

ISSN 2663 - 4023

структури. Таким чином, на вхід кожного ансамблю надходить той самий вектор збудження. Ансамблі розрізняються ефективністю своїх зв'язків. Якщо довжина векторів для всіх ансамблів однакові, то величина збудження ансамблю при незмінному $\Xi$ буде залежати тільки від кутів між $\left(\Xi\hat{}\Phi(0)_{\mu}\right)$ і $\Xi\hat{}\Phi(k)_{\mu}$). Це значить, що максимально збуджується той ансамбль, вектора $\Phi(0)_{\mu}$ та $\Phi(k)_{\mu}$, якого колінеарні вектору $\Xi$. Рішення приймається за номером максимально збудженого ансамблю.

Структура найпростішої нейроподібної системи це набір $M+1$ ансамблів нейронних мереж першого шару. Ансамбль складається з $n$-нейронів, рівень збудження яких визначається як

$$Y_{\mu}(k)=\sum_{a=1}^{n}\Xi a(k)\Phi_{a}(k)_{\mu},$$

Кожен нейрон здійснює кодування процесу, що визначається за, так званим, методом мічених ліній, при якому певним значенням процесу надаються у відповідність визначені (мічені) лінії $Z_1,Z_2,...,Z_a,...,Z_k$ і отже, певному значенню параметра процесу відповідає один максимально збуджений синоптичний зв'язок $\Xi_a(k)=1.$

На відміну від типового нейрона, синоптичні зв'язки якого рівнозначні, у нейрона, що здійснює кодування методом мічених ліній, синоптичні зв'язки мають пріоритет. Синоптичному входу з великим номером відповідає більше значення інформативного параметра процесу. Ще одна відмінність полягає у тому, що у $k$-й момент часу збуджується тільки один синоптичний зв'язок і, тим самим, значно спрощується задача введення й управління порогом $\Theta$, за допомогою вагової функції $w$. Дійсно

$$Y_{\mu}(k)=\sum_{a=1}^{r}\Xi a(k)\Phi_{a}(k)_{\mu}-\Theta_{a}(k)_{\mu}=\sum_{a=1}^{r}\Xi a(k)\Phi_{a}(k)_{\mu}. \qquad (1)$$

При $\Theta_{a}(k)_{\mu}=0$ структура системи, що розпізнає, є квазілінійною, а при $\Theta_{a}(k)_{\mu}\rangle 0$ вона має нелінійні граничні властивості.

Другий шар нейронів в ансамблі реалізує операцію

$$\ln l_{\mu}(k)=\sum_{k=0}^{n}Y_{k}(k). \qquad (2)$$

Він з'єднаний з першим шаром проекційними зв'язками, які встановлюють однозначну відповідність між нейронами різних полів, тобто передають зміни стану з одного поля в інше.

Вхідною інформацією для третього шару нейронів є вектор $\ln L(U)=\left(\ln l_0(U),\ln l_1(U),\ldots,\ln l_m(U)\right).$ Він виконує роль мажоритарного логічного пристрою.

Вирази (1) і (2) цілком визначають структуру системи, що розпізнає стан мережі. Введемо матрицю зв'язків $k$-ї групи сенсорів із $k$-м нейроном, склавши її з індикаторів збудження:

$$\Xi = \begin{pmatrix} \Xi_1 \\ \Xi_1 \\ \cdots \\ \Xi_\kappa \end{pmatrix}. \quad (3)$$

Введемо також поняття коефіцієнта міжнейронного зв'язку *S* в ансамблі (у шарі),

$S_{kl} = \begin{cases} 1, \text{ якщо є : зв'язок між } k\text{-ою групою нейронів.} \\ i \quad \text{якщо існує : 1-й нейрон.} \\ 0, \text{ у зворотному випадку.} \end{cases}$

Утворимо матрицю міжнейронних зв'язків, склавши її з коефіцієнтів міжнейронних зв'язків:

$$S = \begin{pmatrix} S_{00} & S_{01} & \cdots & S_{0n-1} \\ S_{10} & S_{11} & \cdots & S_{1n-1} \\ \cdots & \cdots & \cdots & \cdots \\ S_{n-1} & S_{nn} & \cdots & S_{n-1n-1} \end{pmatrix}, \quad (4)$$

Матриці $\Xi_k$ і *S* цілком визначають структуру зв'язків в ансамблі. Для випадку $Y = 0$ матриця *S* перебудовується в діагональну з розмірністю $n \times n$.

Синтезовані структури припускають фіксований об'єм вибірки, тобто система, що розпізнає, спостерігає відразу всю фазову траєкторію атаки.

Інформаційне поле сприймається сенсорною матрицею у вигляді сукупності спостережень:

$$X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1i} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2i} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{p1} & x_{p2} & \cdots & x_{pi} & \cdots & x_{pn} \end{pmatrix}. \quad (5)$$

Кожен стовпчик $x_i = (x_{i1}, x_{j2}, \ldots, x_{pi}),\ i = 1,2,\ldots,n$ і рядок $x_j = (x_{j1}, x_{j2}, \ldots, x_{jI}),\ j = 1,2,\ldots,p$ матриці *X* є відповідно *n* і *p* – мірні вектора процесів.

Можливі $M+1$ гіпотеза $H_0, H_1, \ldots, H_\mu, \ldots, H_M$ про належність інформаційного поля $\mu$-го класу, що спостерігається. Відомі апріорні ймовірності гіпотез $P = P\{H_\mu\},\quad \mu = 0,1,\ldots,M$. Відома також платіжна матриця:

$$C = \begin{pmatrix} C_{00} & C_{01} & C_{02} & \cdots & C_{0M+1} \\ C_{10} & C_{11} & C_{12} & \cdots & C_{1M+1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ C_{M+10} & C_{M+11} & C_{CM+12} & \vdots & C_{M+1M+1} \end{pmatrix}, \quad (6)$$

елемент $C_{jm}$ якої є платою за рішення $\gamma_\mu$, коли істинною була гіпотеза $H_j$, $j = \mu = 0,1,\cdots,M$. Простір рішень $\Gamma = (\gamma_0, \gamma_2, \ldots, \gamma_M)$ складається з $M+1$ елемента, де $\gamma_\mu$ - рішення прийняти гіпотезу $H_\mu$. Задача системи розпізнавання

заключається в тому, щоб за результатами спостереження прийняти одну з гіпотез і відхилити інші. Середній ризик при ухваленні рішення визначається таким чином:

$$R = \sum_{j=0}^{m}\sum_{\mu=1}^{m} C_{j\mu} P_j \int_{G_\mu} w(x_1, x_2, \ldots, x_m)\, H_0 / X \,. \qquad (7)$$

Мінімальне значення середнього ризику досягається у тому випадку, якщо до області $G_\mu$ ухвалення рішення $\gamma_\mu$ РС віднесе точки X вибіркового простору, що задовольняють системі нерівностей:

$$\sum_{j=1}^{M}\left(C_{ij} - C_{jm}\right)\frac{P_i w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_i}{P_0 w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_0} \geq C_{0\mu} - C_{0j} \,. \qquad (8)$$

Якщо ввести вектор відносин правдоподібності $l(x) = \left[l_0(x), l_1(x), l_\mu(x), \ldots, l_m(x)\right]$,

де $l_\mu = \dfrac{w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_\mu}{w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_0}$, тоді систему нерівностей (8) можна представити у виді:

$$\sum_{j=1}^{M}\left(C_{ij} - C_{jm}\right)\frac{P_i}{P_0} l_i(x) \geq C_{0\mu} - C_{0j} \,. \qquad (9)$$

Вектор $l(x)$ несе всю інформацію про гіпотези, що перевіряються й для ухвалення рішення про результати спостереження досить обчислювати компоненти $M$ - мірного вектора відносин правдивості. Задачу обчислення $l(x)$ й ухвалення рішення в структурі нейророзпізнаючої системи (НРС) вирішує класифікатор.

При рішенні будь-яких задач, пов’язаних із розпізнаванням атак, необхідно попередньо оцінити ступінь відповідності прийнятих параметрів (портретів) еталонним, тобто, визначити критерій ухвалення рішення. Кількісну міру відповідності приходиться вибирати по-різному, у відповідності від характеру проведених досліджень.

Помилкове рішення при функціонування мережі виявляється у тому, що практично знятий портрет однієї атаки буде віднесений до іншого кластера. Якщо помилка є випадковою подією, то вірність ухвалення рішення природно характеризувати ймовірністю відсутності помилки, тобто ймовірністю правильної класифікації. Якщо ймовірність помилки позначимо через $P_{пом}$, то ймовірність правильної класифікації: $P_{\text{пр}} = 1 - P_{\text{пом}}$, тому що помилка і правильна класифікація утворять повну групу подій.

Отже, ІНРС повинна обчислювати відносини правдоподібності, враховувати апріорні ймовірності появи розпізнавальних ДПС і на основі платіжної матриці приймати рішення. Враховуючи незалежність обчислення відносин правдоподібності для кожного кластера, їх можна здійснювати незалежно й паралельно. Ця операція виконується в окремих інформаційно-незалежних ансамблях нейронів. Урахування апріорних ймовірностей появи відповідних дискретно-подійних систем здійснюється нейронним полем урахування апріорних ймовірностей гіпотез. Нейронне поле введення платіжної матриці враховує плату за кожне неправильно прийняте рішення. Мажоритарна мережа виносить рішення про розпізнавання.

В рамках нашого дослідження були сформовані модулі виявлення для окремо взятих атак категорій User-to-Root і Remote-to-Local з тренувальних баз даних KDD, які є найбільш складними для виявлення. Для більшості атак був отриманий результат в 99,8% правильно класифікованих пакетів. Для подібних атак отримані однакові набори «базових» параметрів. При об'єднанні кількох атак одного типу в класи також досягається 99,8% розпізнавання, при цьому збільшується кількість опорних векторів. Процес тестування складався з п'яти етапів. У першій частині тестування використовувалися багаторозрядні параметри трафіку, які добувають із заголовків IP і TCP пакетів. Всього використовувалося 16 базових параметрів, 8 для IP і 8 для TCP. Для значної частини атак було досягнуто 100% розпізнавання. На другому етапі, шляхом поділу багаторозрядних параметрів на кілька частин, кратних 8 бітам, число базових параметрів було збільшено до 28. В результаті аналогічного тестування для більшого числа атак було досягнуто 97,6% розпізнавання. У порівнянні з багаторозрядними параметрами збільшилася кількість опорних векторів, і велику роль став грати вибір даної матриці в методі головних компонент.

На третьому етапі тестування в набір розглянутих базових параметрів були включені статистичні параметри TCP-сеансів: час з'єднання, число переданих і прийнятих пакетів, байт і число пакетів з різними мітками - всього 38 базових параметрів. Для всіх розглянутих атак істотно збільшилася кількість опорних векторів, що викликано збільшенням розрядності простору. Для певного типу атак так і не було отримано 100% результат. Для деяких атак виявилося досить від 3 до 8 нових параметрів з 38 для досягнення 100% розпізнавання та незначного збільшення числа опорних векторів. На четвертому етапі для атак, які не вдавалося виявити на попередніх етапах, була проведена кластеризація тренувальних даних і проведені процедури навчання нових модулів виявлення. На п'ятому етапі було реалізовано розширення можливостей блоків кластеризації і класифікацій шляхом внесення нечіткості. В результаті побудовані пересічні кластери, однакові пакети з різними мітками були віднесені до класу атак з певною ймовірністю. За результатами експериментальних досліджень був створений програмний прототип який показав, що поєднання нейромережевих структур розпізнавання з методом скорочення розмірності дав ймовірність правильного виявлення атаки 96,4, з методом кластеризації – 97,8. Метод опорних векторів із застосуванням нейромережевої структури розпізнавання підвищив показники виявлення для окремих модулів до 99,6% (чисто нейромережева система розпізнавання мала показник 92,4%) .

## 3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене експериментальне дослідження підтвердило правильність запропонованої моделі та вибору безлічі методів інтелектуального розподілу даних, що лежать в її основі. Метод опорних векторів в поєднанні з нейромережевою структурою розпізнавання дозволив ідентифікувати більшість атак з результатом 99,6%.

Таким чином в статті запропоновано побудова системи виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних і проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту інформаційної мережі.

Проведені експерименти показали високу якість виявлення мережевих атак і довели правильність вибору методів інтелектуального аналізу даних і застосовність вироблених методик. Застосування різних методів, можливість настройки внутрішніх

параметрів і порогових значень дозволяють домогтися оптимального співвідношення продуктивності системи і точності розпізнавання атак в інформаційній мережі.

Подальші дослідження можуть бути направлені на комбінаторику застосування методів інтелектуального розподілу даних з іншими відомими методами та системами виявлення вторгнень.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Хакерські атаки в Україні. [Електронний ресурс] // Вікіпедія : [сайт]. Київ, 2020. https://glavcom.ua/topics/ rosijskikhakeru.html.

[2] Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, А. В. Котенко // Тр. СПИИРАН. 2016. № 2 (45). С. 207-244.

[3] Сучасні методи виявлення аномалій в системах виявлення вторгнень / О.М. Колодчак // Вісник Національного ун-т «Львівська політехніка». Комп'ютерні системи та мережі. 2012. № 745. С. 98-104.

[4] Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д. О. Даниленко, О. А. Смірнов, Є. В. Мелешко // Системи озброєння і військова техніка. Х.: Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, 2012. № 1. С. 92-100.

[5] The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014.

[6] Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак / Г.Бекетова, Б. Ахметов, О. Корченко, В. Лахно // Безпека інформації. К: НАУ, 2016. Т. 22, № 3. С. 242-254.

[7] Огляд систем виявлення атак в мережевому трафіку / К. М. Носенко, О. І. Півторак, Т. А. Ліхоузова // Адаптивні системи автоматичного управління. К: НТУУ КПІ, 2014. № 1 (24). С. 67-75.

[8] Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. Computer Network and Information Security, 2014. Vol. 8. 41-47 pp.

[9] Аналіз сучасних систем виявлення атак і запобігання вторгненням / А. А.Завада, О. В. Самчишин, В. В. Охрімчук // Інформаційні системи. Житомир: Збірник наукових праць ЖВІ НАУ, 2012. Т. 6, № 12. С. 97-106.

[10] An implementation of intrusion detection system using genetic algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Network Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, No. 2. P. 109-120.

[11] Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, No. 2. P. 169-184.

[12] IDS / IPS. Netgate Documentation: [website]. Washington: Rubicon Communications LLC, 2017. [Electronic resource]. Online: https://www.netgate. com/docs/pfsense/ids-ips/.

[13] Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Науково-технічний журнал "Сучасний захист інформації".– №1. 2019. С. 56-62.

[14] Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). c. 69-79.

[15] DARPA Intrusion Detection Data Sets [Электронный ресурс] — Режим доступа: https://www.ll.mit.edu/ideval/data/.

[16] KDD Cup 1999 Data [Электронный ресурс] — Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99.

[17] Kayacik, H. G. Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets / H. G. Kayacik, A. N. Zincir-Heywood, M. I. Heywood // Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST-2005) — 2006. — P. 85–89.

[18] Haykin, S. Neural Networks and Learning Machines / S. Haykin // Pearson Education, 2009. — 937 p.

[19] Cannady, J. Applying CMAC-based On-line Learning to Intrusion Detection / J. Cannady // In: Proc. of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. — 2000. — Vol. 5 — P. 405–410.

[20] Lee, S. C., Heinbuch, D. V. Training a neural-network based intrusion detector to recognize novel attacks / S. C. Lee, D. V. Heinbuch // IEEE Transactions on Systems, Man, and Cybernetics: Part A — 2001. — Vol. 31. — No. 4. — P. 294–299.

[21] Liu, G. A hierarchical intrusion detection model based on the PCA neural networks / G. Liu, Z. Yi, S. Yang // Neurocomputing 70. — 2007 — Vol. 7. — No. 9. — P. 1561–1568.

[22] Parlos, A. Application of the recurrent multilayer perceptron in modeling complex process dynamics / A. Parlos, K. Chong, A. Atiya // IEEE Transactions on Neural Networks. — 1994. — Vol. 5. — No. 2. — P. 255–266.

[23] Hsu, C-W. A Practical Guide to Support Vector Classification / C-W. Hsu, C-C. Chang, C-J. Lin — Department of Computer Science, National Taiwan University, Taipei 106, Taiwan, 2003. — 16 p.

[24] Miguel, A. Carreira-Perpinan A Review of Dimension Reduction Techniques / A. Carreira-Perpinan Miguel. — Technical Report CS-96-09 Dept. of Computer Science University of Sheffield, 1997. — 69 p.

[25] Fodor, I. K. A Survey of Dimension Reduction Techniques / I. K. Fodor — U.S. Department of Energy by University of California, Lawrence Livennore National Laboratory, 2002. — 26 p.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

**Serhii Toliupa**
Doctor of Technical Sciences, Professor, Professor of Cybersecurity and Information Security
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0000-0002-1919-9174
*tolupa@i.ua*

**Oleksandr Pliushch**
PhD in technical sciences, docent, professor of the department of Mobile and video information technologies
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0001-5310-0660
*opliusch@yahoo.com*

**Ivan Parkhomenko**
PhD, Associate Professor, Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kiev
ORCID: 0000-0001-6889-9284
*parkh08@ukr.net*

# CONSTRUCTION OF ATTACK DETECTION SYSTEMS IN INFORMATION NETWORKS ON NEURAL NETWORK STRUCTURES

**Abstract.** Systems for detecting network intrusions and detecting signs of attacks on information systems have long been used as one of the necessary lines of defense of information systems. Today, intrusion and attack detection systems are usually software or hardware-software solutions that automate the process of monitoring events occurring in an information system or network, as well as independently analyze these events in search of signs of security problems. As the number of different types and ways of organizing unauthorized intrusions into foreign networks has increased significantly in recent years, attack detection systems (ATS) have become a necessary component of the security infrastructure of most organizations.
The article proposes a software prototype of a network attack detection system based on selected methods of data mining and neural network structures. The conducted experimental researches confirm efficiency of the created model of detection for protection of an information network. Experiments with a software prototype showed high quality detection of network attacks based on neural network structures and methods of intelligent data distribution. The state of protection of information systems to counter cyber attacks is analyzed, which made it possible to draw conclusions that to ensure the security of cyberspace it is necessary to implement a set of systems and protection mechanisms, namely systems: delimitation of user access; firewall; cryptographic protection of information; virtual private networks; anti-virus protection of ITS elements; detection and prevention of intrusions; authentication, authorization and audit; data loss prevention; security and event management; security management.

**Keywords:** cyberspace, attack, neural network, information network, attack detection systems, data mining methods, training base, fuzzy logic, cauterization, cyber defense.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Hacker attacks in Ukraine. [Electronic resource] // Wikipedia: [site]. Kyiv, 2020. https://glavcom.ua/topics/ rosijskikhakeru.html.
[2] Analysis and classification of methods for detecting network attacks / AA Branitsky, AV Kotenko // Tr. SPIIRAN. 2016. № 2 (45). Pp. 207-244.
[3] Modern methods of detecting anomalies in intrusion detection systems / O.M. Kolodchak // Bulletin of the National University "Lviv Polytechnic". Computer systems and networks. 2012. № 745. pp. 98–104.
[4] Research of methods of detection of intrusions into telecommunication systems and networks / DO Danilenko, OA Smirnov, EV Meleshko // Weapons systems and military equipment. H .: Hark. nat. University of the Air Force. I. Kozheduba, 2012. № 1. S. 92-100.

[5] The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014.
[6] Development of a model of intelligent recognition of anomalies and cyberattacks using logical procedures based on feature matrix coatings / G. Beketova, B. Akhmetov, O. Korchenko, V. Lakhno // Information Security. K: NAU, 2016. T. 22, № 3. S. 242-254.
[7] Review of attack detection systems in network traffic / KM Nosenko, OI Pivtorak, TA Likhouzova // Adaptive automatic control systems. K: NTUU KPI, 2014. № 1 (24). Pp. 67-75.
[8] Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. Computer Network and Information Security, 2014. Vol. 8. 41-47 pp.
[9] Analysis of modern systems for detecting attacks and preventing invasion / AA Zavada, OV Samchyshyn, VV Okhrimchuk // Information systems. Zhytomyr: Collection of scientific works of ZhVI NAU, 2012. T. 6, № 12. S. 97-106.
[10] An implementation of intrusion detection system using genetic algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Network Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, no. 2. P. 109-120.
[11] Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, no. 2. P. 169-184.
[12] IDS / IPS. Netgate Documentation: [website]. Washington: Rubicon Communications LLC, 2017. [Electronic resource]. Online: https: //www.netgate. com / docs / pfsense / ids-ips /.
[13] Dovbeshko SV, Tolyupa SV, Shestak Ya.V. Application of data mining methods to build attack detection systems. Scientific and technical journal "Modern information protection". - "1. 2019. S. 56-62.
[14] Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). with. 69-79.
[15] DARPA Intrusion Detection Data Sets [Electronic resource] - Access mode: https://www.ll.mit.edu/ideval/data/.
[16] KDD Cup 1999 Data [Electronic resource] - Access mode: http://kdd.ics.uci.edu/databases/kddcup99.
[17] Kayacik, HG Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets / HG Kayacik, AN Zincir-Heywood, MI Heywood // Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST- 2005) - 2006. - P. 85–89.
[18] Haykin, S. Neural Networks and Learning Machines / S. Haykin // Pearson Education, 2009. - 937 p.
[19] Cannady, J. Applying CMAC-based On-line Learning to Intrusion Detection / J. Cannady // In: Proc. of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. - 2000. - Vol. 5 - P. 405–410.
[20] Lee, S. C., Heinbuch, D. V. Training a neural-network based intrusion detector to recognize novel attacks / S. C. Lee, D. V. Heinbuch // IEEE Transactions on Systems, Man, and Cybernetics: Part A - 2001. - Vol. 31. - No. 4. - P. 294–299.
[21] Liu, G. A hierarchical intrusion detection model based on the PCA neural networks / G. Liu, Z. Yi, S. Yang // Neurocomputing 70. - 2007 - Vol. 7. - No. 9. ó P. 1561–1568.
[22] Parlos, A. Application of the recurrent multilayer perceptron in modeling complex process dynamics / A. Parlos, K. Chong, A. Atiya // IEEE Transactions on Neural Networks. - 1994. - Vol. 5. - No. 2. - P. 255–266.
[23] Hsu, C-W. A Practical Guide to Support Vector Classification / C-W. Hsu, C-C. Chang, C-J. Lin - Department of Computer Science, National Taiwan University, Taipei 106, Taiwan, 2003. - 16 p.
[24] Miguel, A. Carreira-Perpinan A Review of Dimension Reduction Techniques / A. Carreira-Perpinan Miguel. - Technical Report CS-96-09 Dept. of Computer Science University of Sheffield, 1997. - 69 p.
[25] Fodor, I. K. A Survey of Dimension Reduction Techniques / I. K. Fodor - U.S. Department of Energy by University of California, Lawrence Livennore National Laboratory, 2002. - 26 p.