УДК 004.056.53

Р.В. Грищук,
доктор технічних наук, старший науковий співробітник
В.М. Мамарєв

АНАЛІЗ ЕФЕКТИВНОСТІ АЛГОРИТМІВ КЛАСИФІКАЦІЇ КІБЕРАТАК

У статті розкрито технологію аналізу ефективності алгоритмів класифікації кібератак.

Ключові слова: *алгоритм, класифікація, кібератака, ефективність, точність, критерій.*

В статье раскрыта технология анализа эффективности алгоритмов классификации кибератак.

Ключевые слова: *алгоритм, классификация, кибератака, эффективность, точность, критерий.*

The results of the analysis of the effectiveness of classification algorithms of cyberattacks is given in the paper.

Keywords: *algorithm, classification, cyberattack, efficiency, accuracy criterion.*

В основу роботи більшості відомих систем виявлення атак (СВА) покладено технологію сигнатурного аналізу, яка реалізується на основі відповідних алгоритмів класифікації [1–3]. При цьому алгоритми класифікації кібератак різняться між собою як за точністю класифікації кібератак, так і за способом реалізації цих алгоритмів. Суттєві вимоги висуваються також до набору параметрів потоку вхідних даних, що підлягають аналізу та подальшій класифікації. Недосконаліть відомих методик аналізу ефективності алгоритмів класифікації кібератак обмежує вибір найефективнішого алгоритму через відсутність загальноприйнятих критеріїв. Тому завдання аналізу ефективності алгоритмів класифікації кібератак за показниками точності класифікації шаблонів атак (ША) та шаблонів нормальної поведінки (ШНП) на основі уніфікованого набору вхідних даних та єдиної програмної платформи для реалізації алгоритмів є актуальним як ніколи.

Аналіз останніх досліджень і публікацій [1–5] показує, що основу модуля класифікації в СВА складають алгоритми, які ґрунтуються на лінійних, логічних комбінаторно-логічних, статистичних, нейромережевих та гібридних методах класифікації. З аналізу літератури [4, 6, 7] та ін. встановлено, що, незважаючи на переваги наведених методів, кожен з них має ряд недоліків, котрі, як наслідок, вливають на якість класифікації. Наприклад, недоліком методу опорних векторів є класифікація з використанням незначної граничної частини даних. До недоліків методу "найближчого сусіда" відносять необхідність повного перебору навчальної вибірки і складність вибору міри "подібності". Застосування байєсівських методів вимагає приведення неперервних даних до інтервальної шкали тощо. Тому процедура аналізу ефективності алгоритмів класифікації кібератак з урахуванням виявлених недоліків потребує подальшого удосконалення.

Метою статті є аналіз ефективності алгоритмів класифікації кібератак за показниками точності класифікації ША та ШНП на основі уніфікованого набору вхідних даних та єдиної програмної платформи.

Оберемо як вихідні такі критерії аналізу ефективності алгоритмів класифікації: точність класифікації ША та ШНП; єдина програмна платформа реалізації алгоритмів; використання уніфікованого набору вхідних даних. Для забезпечення коректності проведення процедури аналізу також доцільно організувати додержання вимоги щодо ідентичності конфігурації обчислювальних засобів.

Нехай точність класифікації ША та ШНП визначатиметься за певним критерієм згідно з виразом:

$$Accuracy = \frac{TP + TN}{2} \times 100\% \ , \qquad (1)$$

де TP – точність класифікації ШНП;

TN – точність класифікації ША.

З урахуванням обраного критерію (1) для відомих алгоритмів класифікації кібератак, що аналізуються, і відповідних їм показників точності у табл. 1 подамо результати верифікації алгоритмів за критерієм “точність класифікації”.

Таблиця 1

Результати верифікації алгоритмів класифікації за критерієм точність класифікації

Алгоритм класифікації	Точність класифікації згідно з [11]		Критерій точності (1)
	TP	*TN*	*Accuracy*
Naive Bayes	0,9364	0,8663	90,3829
Bayes Net	0,9935	0,9466	97,1708
SVM	0,9856	0,9608	97,405
MLP	0,9929	0,9777	99,7658
IBK	0,9977	0,9972	99,7452
Decision Table	0,9977	0,992	99,5015
JRip	0,9986	0,9973	99,8039
OneR	0,942	0,9878	96,3318
J48	0,9979	0,9977	99,7817
NB Tree	0,9991	0,9984	99,8746
Random Tree	0,9979	0,9974	99,7658
Random Forest	0,9996	0,9982	99,8968
REP Tree	0,9986	0,998	99,8357

На рис. 1 подамо результати ранжування досліджуваних алгоритмів класифікації кібератак (див. табл. 1) за критерієм точність класифікації.

Цифри на рис. 1 визначають місце досліджуваного алгоритму. Результати ранжування дозволяють зробити висновок про те, що при застосуванні функції перехресної перевірки з параметром розбиття – 10 найкращу точність класифікації ШНП та ША мають алгоритми групи, які ґрунтуються на математичному апараті побудови дерев прийняття рішень. При цьому найгірші показники класифікації за точністю має *алгоритм наївної Байєсовської класифікації*, найкращі – *J48* та *Random Forest*. Алгоритм *J48* точніше класифікує ШНП, *Random Forest* – ША.

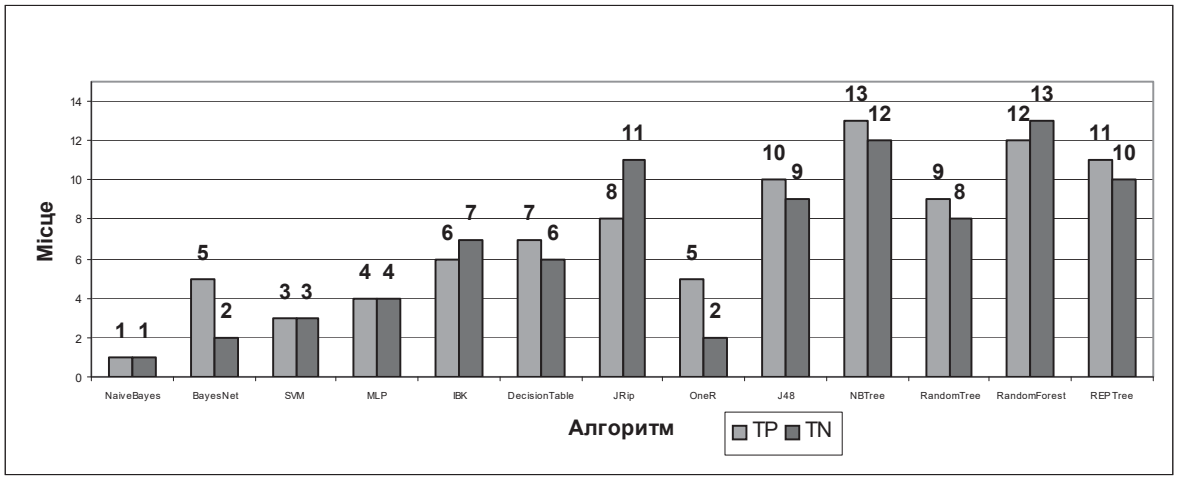

Рис. 1. Результати ранжування алгоритмів класифікації кібератак за критерієм точність класифікації

Для виконання умови щодо застосування єдиної програмної платформи реалізації алгоритмів скористаємося розробленою університетом Уайкато системою аналізу даних (САД) *Weka* [8]. *Weka* є бібліотекою програм, що реалізують лінійні, комбінаторно-логічні, статистичні, нейромережеві, гібридні методи прогнозу, класифікації та здобуття знань, а також колективні методи прогнозу та класифікації. Бібліотека алгоритмів *Weka* забезпечує можливість доступу до алгоритмів, ефективність яких аналізується (див. табл. 1).

Уніфікованість та доступність набору вхідних даних при аналізі ефективності забезпечено використанням групи баз станів системи *NSL-KDD*. Структурно *NSL-KDD* складається з двох навчальних *KDDTrain+* та *KDDTrain+20Percent* й двох тестових *KDDTest+*та *KDDTest-21* баз станів. Порівняно з *KDD99,* база *NSL-KDD* [9] має ряд переваг. Наприклад: в навчальному та тестовому наборах станів системи виключені надлишкові записи, що забезпечує одержання не зміщених результатів класифікації; кількість обраних записів для кожної з груп визначеного рівня складності в тестових наборах даних обернено пропорційна відсотку записів у оригінальній базі, що забезпечує більш точні оцінки алгоритмів класифікації; зменшення кількості записів у навчальних та тестових наборах дозволяє проводити експерименти без потреби розбиття вхідного потоку даних. Визначені переваги бази *NSL-KDD* дозволяють забезпечити коректність порівняння оцінок ефективності алгоритмів класифікації кібератак.

Ідентичність конфігурації обчислювальних засобів в роботі забезпечена використанням ПЕОМ з такими технічними параметрами: ОС *Windows 7 Ultimate SP1 (x64)*; процесор *Pentium (R) Dual-Core T4300@ 2.10GHz 2.10GHz*; ОЗП *2,00 Gb*.

Аналіз ефективності алгоритмів класифікації проводився в чотири етапи. Його сутність полягала в такому.

На першому етапі з використанням навчальної бази *KDDTrain+* в САД *Weka* для кожного з досліджуваних алгоритмів було розроблено модель, проведено її навчання та верифікацію. Тестовий набір станів системи формувався шляхом використання вбудованої функції перехресної перевірки (*Cross-validation*) з параметром розбиття – 10. Тобто перед початком роботи програми база *KDDTrain+*

була автоматично розділена у відношенні 9 до 1 на навчальну і тестову відповідно. Потім на 9 частинах проводиться навчання моделі, а частина, що залишилася, використовувалася для тестування. Процедура повторювалася 10 разів. Як наслідок, кожна з 10 частин даних використовувалася для тестування. У результаті одержано оцінку ефективності досліджуваного алгоритму за обраним критерієм.

Другий етап передбачає здійснення верифікації (верифікації побудованих моделей з використанням бази *KDDTest+*). Результати верифікації подано в табл. 2.

Таблиця 2

Результати верифікації алгоритмів класифікації за критерієм точність класифікації на навчальній базі *KDDTest+*

Назва алгоритму класифікації	Точність класифікації згідно з [11]		Критерій точності (1)
	TP	*TN*	*Accuracy*
Naive Bayes	0,931	0,6327	76,1178
Bayes Net	0,973	0,5713	74,4322
SVM	0,9246	0,6248	75,3948
MLP	0,9283	0,6549	81,3565
IBK	0,962	0,6661	79,3559
Decision Table	0,9736	0,5385	72,5958
JRip	0,9719	0,6246	77,4219
OneR	0,9573	0,7052	81,3786
J48	0,9729	0,6961	81,5339
NB Tree	0,9124	0,6906	78,6107
Random Tree	0,9206	0,7326	81,3565
Random Forest	0,9295	0,6628	77,7679
REP Tree	0,9093	0,7438	91,5073

Проаналізувавши діаграму, можна зробити висновок, що найкращі показники класифікації ШНП має алгоритм *Decision Table*, ША – *REPTree*. Однак показники класифікації іншого шаблону (ША для *Decision Table*, ШНП для *REPTree*) є незадовільно низькими. Оптимальні значення одночасної точності класифікації ШНП і ША показав алгоритм *J48*.

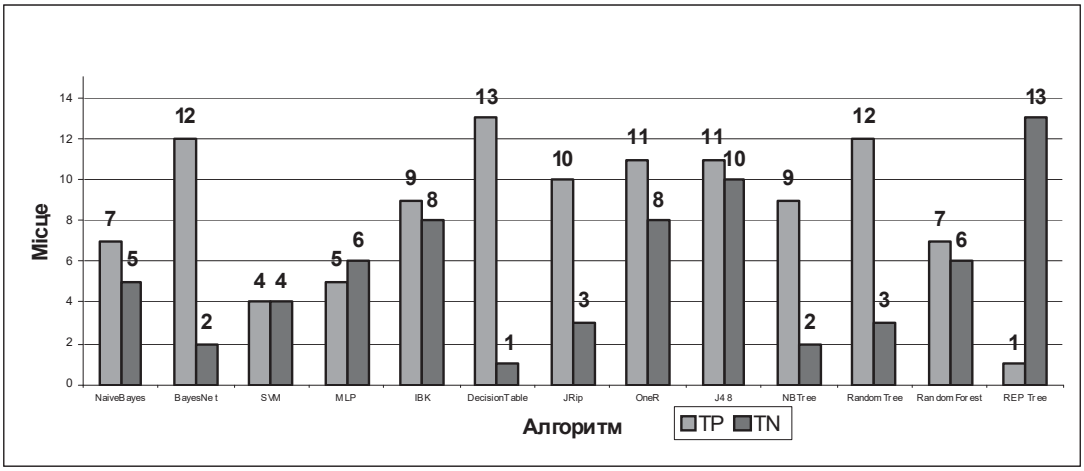

Рис. 2. Результат ранжування алгоритмів класифікації за точністю класифікації ША та ШНП на основі KDDTest+

На третьому етапі алгоритми верифіковано з використанням тестової бази *KDDTest-21*. Детальний аналіз бази *KDDTest+* дозволив встановити, що з 22544 шаблонів поведінки такі алгоритми, як *J48*, *NaiveBayes*, *NBTree*, *RandomForest*, *RandomTree*, *Multilayer Perceptron* та *SVM* правильно класифікують не менше 10694 шаблонів, тобто 47,4% від загальної кількості. Тому тестову базу KDDTest-21 було сформовано шляхом вилучення з тестового набору *KDDTest+* зазначених записів. Результати верифікації алгоритмів класифікації з використання бази шаблонів поведінки системи *KDDTest-21* подано в табл. 3.

Таблиця 3

Результати верифікації алгоритмів класифікації за критерієм точність класифікації на навчальній базі KDDTest-21

Назва алгоритму класифікації	Точність класифікації згідно з [11]		Критерій точності (1)
	TP	*TN*	*Accuracy*
Naive Bayes	0,691	0,5173	54,8861
Bayes Net	0,8783	0,4339	51,4599
SVM	0,6673	0,5035	53,3249
MLP	0,6784	0,5433	64,7764
IBK	0,8309	0,5582	60,7679
Decision Table	0,8838	0,3896	47,9325
JRip	0,8745	0,5034	57,0802
OneR	0,8545	0,6101	64,4008
J48	0,8796	0,5979	64,903
NB Tree	0,6264	0,5905	59,7046
Random Tree	0,6185	0,661	64,7764
Random Forest	0,6822	0,5538	57,7131
REP Tree	0,6473	0,6479	65,3249

Графік, що відображає ранги алгоритмів за точністю класифікації шаблонів ШНП та ША, подано на рис. 3.

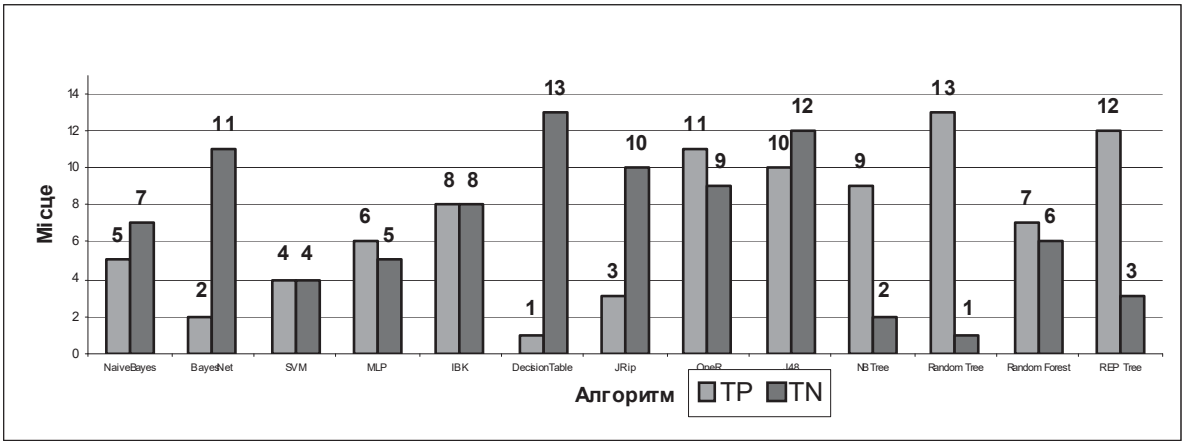

Рис. 3. Результат ранжування алгоритмів за точністю класифікації ША та ШНП на основі KDDTest^{-21}

Верифікація алгоритмів класифікації кібератак з використанням бази шаблонів поведінки системи *KDDTest-21* показала, що найкращі показники класифікації мають алгоритми *Random Tree* та *REP Tree* – для ШНП, ША – *Decision Table, J48*. Оп-

тимальні значення одночасної точності класифікації ШНП і ША також має алгоритм *J48*.

Четвертий етап аналізу ефективності алгоритмів класифікації полягав у визначенні найбільш ефективного алгоритму за результатами оцінювання точності одержаних на попередніх етапах. Найбільш ефективний алгоритм визначався шляхом визначення сумарного місця за результатами розрахунків, отриманих на перших трьох етапах дослідження за кожним з обраних критеріїв ефективності.

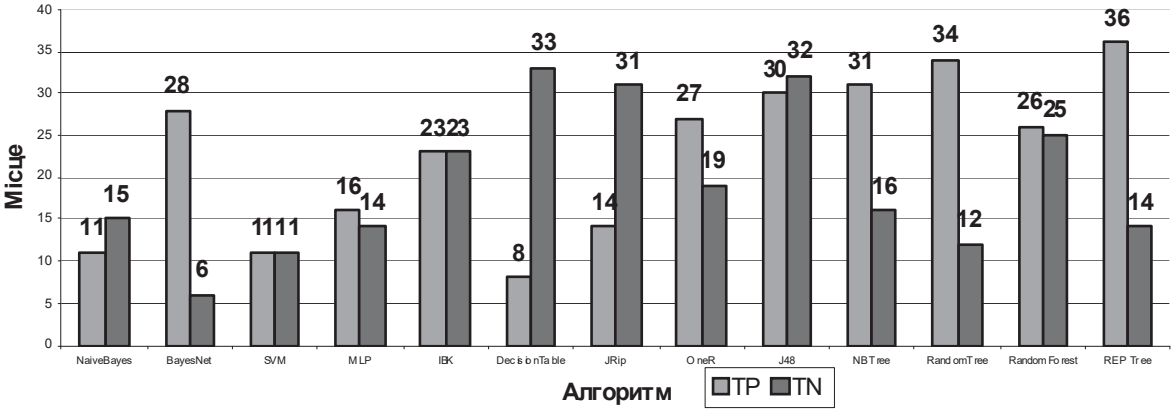

Рис. 4. Результати аналізу ефективності алгоритмів класифікації кібератак

Аналіз результатів оцінювання ефективності алгоритмів класифікації кібератак показує, що вони суттєво різняться за здатністю класифікації шаблонів стану системи. Точність класифікації шаблонів поведінки системи з використанням тестових баз також є різною. Це пов'язано з різною складністю подання записів в базах даних. Так, наприклад, алгоритм *REPTree* найбільш ефективно здійснює класифікацію ША, однак має відносно низьку ефективність виявлення ШНП. Найкращі показники ефективності має алгоритм класифікації *J48*, що показав однаково високі показники виявлення ША та ШНП. Таким чином, створюючи інтелектуальну СВА, слід, у першу чергу, орієнтуватися на використання в ній алгоритму класифікації кібератак *J48* як такого, що є найбільш ефективним порівняно з відомими.

Таким чином, у роботі вперше наведено результати аналізу ефективності алгоритмів класифікації кібератак з використанням уніфікованого набору вхідних даних *NSL-KDD* та єдиної програмної платформи реалізації алгоритмів – САД Weka. Як наслідок, встановлено, що досліджені алгоритми не інваріантні до тестових баз даних. Тому напрямом подальших досліджень буде вибір та адаптація досліджених алгоритмів для підвищення ефективності класифікації станів системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Ленков С.В.* Методы и средства защиты информации : монография : в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Т. 2. Информационная безопасность. – К. : Арий, 2008. – 344 с.

2. *Грищук Р.В.* Постановка задачі розробки методики скорочення розмірності потоку вхідних даних для мережних систем виявлення атак / Р.В. Грищук, В.М. Мамарєв // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля, 2011. – № 1(5). – С. 74–78.

3. *Грищук Р.В.* Диференціально-ігрова модель нормальної поведінки Web-сервера / Р.В. Грищук. – 2010. – № 212. – С. 96–106 [Електронний ресурс]. – Режим доступу : http : // pt.journal.kh.ua/2010/2/2/102_gryschuk_web.pdf.

4. *Грищук Р.В.* Диференціально-ігрова модель шаблону атаки на Web-сервер / Р.В. Грищук // зб. наук. пр. ВІКНУ ім. Т.Г. Шевченка. – К. : ВІКНУ ім. Т.Г. Шевченко, 2010. – № 21. – С. 104–112.

5. *Дуда Р.* Распознавание образов и анализ сцен / Р. Дуда, П. Харт. – М. : Мир, 1976. – 512 с.

6. Технологии анализа данных : Data Mining, Visual Mining, Text Mining, OLAP/ А.А. Барсегян, М.С. Куприянов, В.В. Степаненко, И.И. Холод. – 2-е издание, перераб. и допол. – СПб. : БХВ-Петербург, 2007. – 384 с.

7. *Чубукова И.А.* Data Mining: учебное пособие / И.А. Чубукова. – М. : БИНОМ, 2006. – 382 с.

8. Weka data mining software [Електронний ресурс]. – Режим доступу : http : //www.cs.waikato.ac.nz/ml/weka/index.html.

9. Прикладная статистика. Классификация и снижение размерности / С.А. Айвазян, В.М. Бухштабер, И.С. Ешоков та ін. – М. : ФиС, 1989. – 607 с.

10. *Осовский С.* Нейронные сети для обработки информации / С. Осовский ; пер. с пол. И.Д. Рудинского. – М. : Финансы и статистика, 2002. – 344 с.

11. The NSL-KDD Data Set [Електронний ресурс]. – Режим доступу : http : // nsl.cs.ca/NSL-KDD.

12. UCI Knowledge Discovery in Databases Archive [Електронний ресурс]. – Режим доступу : http : // kdd.ics.uci.edu.

Отримано 5.09.2014

Рецензент Рибальський О.В., доктор технічних наук, професор.