ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.738.5:004.056.5(045)

Р. В. Грищук, В. М. Мамарєв, К. В. Молодецька-Гринчук

КЛАСИФІКАЦІЯ ПРОФІЛІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АКТОРІВ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ (НА ПРИКЛАДІ МІКРОБЛОГУ TWITTER)

Житомирський військовий інститут ім. С. П. Корольова, Житомир

Національний центр управління та випробувань космічних засобів, Київ

Житомирський національний агроекологічний університет, Житомир

Анотація. Соціальні інтернет-сервіси (СІС) представляють собою популярний засіб соціальної комунікації учасників віртуальних спільнот – акторів. Одночасно СІС перетворилися на ефективний інструмент проведення інформаційних операцій, спрямованих проти інформаційної безпеки держави. Тому важливим науковим завданням є своєчасне виявлення ознак інформаційних операцій у СІС. На попередніх етапах досліджень розроблено метод побудови профілів інформаційної безпеки акторів у СІС, який дозволяє оцінити рівень їх загрози як можливого учасника інформаційної операції. Запропонований метод узагальнений на всі СІС і не враховує різноманітність набору атрибутів профілів у окремих сервісах. Отже, перспективним напрямком досліджень є адаптація даного методу для конкретного СІС і його верифікація для подальшого використання у системі забезпечення інформаційної безпеки держави. У статті виконано експериментальне дослідження методу на прикладі мікроблогу Twitter. Встановлено, що точність та швидкодія побудови профілів залежить від алгоритму бінарної класифікації, який застосовується на етапі віднесення актора до одного із заданих класів загроз. Отримані результати збіжні з відомими академічними дослідженнями, що свідчить про доцільність застосування розробленого методу для автоматизації процедур раннього виявлення ознак інформаційних операцій у СІС.

Ключові слова: соціальний інтернет-сервіс, актор, інформаційна безпека, машинне навчання, бінарна класифікація, загрози, оцінювання.

Аннотация. Социальные интернет-сервисы (СИС) представляют собой популярное средство социальной коммуникации участников виртуальных сообществ – акторов. Одновременно СИС превратились в эффективный инструмент проведения информационных операций, направленых против информационной безопасности государства. Поэтому важной научной задачей является своевременное выявление признаков информационных операций в СИС. На предыдущих этапах исследований разработан метод построения профилей информационной безопасности акторов в СИС, который позволяет оценить уровень их угрозы как возможного участника информационной операции. Предложенный метод обобщен на все СИС и не учитывает разнообразие набора атрибутов профилей в отдельных сервисах. Итак, перспективным направлением исследований является адаптация данного метода для конкретного СИС и его верификация для дальнейшего использования в системе обеспечения информационной безопасности государства. В статье выполнено экспериментальное исследование метода на примере микроблога Twitter. Установлено, что точность и быстродействие построения профилей зависит от алгоритма бинарной классификации, который применяется на этапе отнесения актора к одному из заданных классов угроз. Полученные результаты совпадают с известными академическими исследованиями, что свидетельствует о целесообразности применения разработанного метода для автоматизации процедур раннего выявления признаков информационных операций в СИС.

Ключевые слова: социальный интернет-сервис, актор, информационная безопасность, машинное обучение, бинарная классификация, угрозы, оценивание.

Abstract. Social networking services (SNS) are a popular means of social communication for members of virtual communities - actors. At the same time, SNS have become an effective tool for conducting information operations directed against state information security. Therefore, an important scientific task is the timely detection of signs of information operations in the SNS. In the previous stages of research, a method for constructing profiles of information security actors in the SNS, which allows to assess the level of their threat as a possible participant in the information operation. The proposed method is generalized to all SNS and does not take into account the diversity of the set of attributes of profiles in individual services. Consequently, the perspective direction of research is the adaptation of this method for a specific SNS and its verification for further use in the system of providing information security of the state. An experimental study of the method is performed on the example of the microblogging Twitter. It is established that the accuracy and speed of the construction of profiles depends on the algorithm of the binary classification, which is used at the stage of assigning the actor to one of the given classes of threats. The obtained results coincide with the known academic studies, which testifies to the expediency of application of the developed method for automation of procedures for early detection of signs of information operations in the SNS.

Key words: social networking service, actor, information security, machine learning, binary classification, threats, evaluation.

Вступ

Соціальні інтернет-сервіси (СІС) нині перетворилися на ефективну контент-платформу, яка об'єднує учасників віртуальних спільнот – акторів у групи за їх інтересами [1, 2]. Інколи такими інтересами стають питання державотворення, які в свою чергу нерозривно пов'язані з інформаційною безпекою людини, суспільства та держави. Останнім часом СІС де-факто стають інструментом інформаційних операцій [3], оскільки в них цілеспрямовано поширюється недостовірний або викривлений контент. Наприклад, під час гібридної війни в Україні у мікроблозі *Twitter* агресором, колабораціоністами та їх прибічниками поширювався контент з метою маніпулювання суспільною думкою акторів, нарощування суспільної напруженості, зростання протестних настроїв, спонукання до міжнаціональної ворожнечі [3, 4]. Тому одним із важливих завдань, які покладаються на систему забезпечення інформаційної безпе-

ки держави, є своєчасне виявлення ознак інформаційних операцій, у тому числі й тих, що використовують як інструмент СІС.

Актуальність

Аналіз останніх досліджень і публікацій [5–8] показав відсутність загальноприйнятих методик аналізу профілів акторів у СІС. Відомо [3], що профіль актора у СІС і розроблений або поширюваний ним контент є одним з джерел інформації про його власника. Тому зазвичай, як показано в [9], встановлення профіля інформаційної безпеки актора в СІС виконується засобами методів машинного навчання, що дозволяє проводити класифікацію профілів акторів за різними ознаками [6]. У публікації [9], яка ґрунтується на дослідженнях *M. Pennacchiotti* та *A. M. Popescu* [7], запропоновано оцінювати профіль інформаційної безпеки актора, а саме рівень його загрози як можливого учасника інформаційних акцій на основі агрегування характеристик профіля в СІС. Розроблений підхід до побудови профілів інформаційної безпеки акторів узагальнений на різні види СІС. Але при цьому він не враховує різноманітність набору атрибутів профілів у окремих СІС, зокрема обмеженість інформації про актора і відсутність віртуальних спільнот у деяких сервісах, наприклад *Twitter*. З метою усунення виявлених протиріч в [9] запропоновано відносити актора до одного із попередньо заданих класів загрози, суть якого полягає у оцінюванні характеристик профілю актора у СІС за категоріями: атрибути профілю актора; активність публікації актором контенту; лінгвістичні ознаки контенту актора; зв'язки актора з учасниками віртуальної спільноти. Але на практиці даний метод потребує верифікації та адаптації для конкретного виду СІС залежно від набору атрибутів профілю актора, який використовується у ньому. Тому перспективним напрямком досліджень є адаптація методу побудови профілів інформаційної безпеки акторів для конкретного СІС і його верифікація для подальшого використання у системі забезпечення інформаційної безпеки держави.

Мета

Метою статті є класифікація профілів інформаційної безпеки акторів у СІС для практичного застосування відповідних методів завчасного виявлення ознак інформаційних операцій.

Задачі

1. Обґрунтувати вибір набору вхідних даних для класифікації профілів інформаційної безпеки акторів у СІС.

2. Провести експериментальне дослідження методу побудови профілів інформаційної безпеки акторів із врахуванням особливостей функціонування обраного СІС.

Вибір вхідних даних для класифікації профілів інформаційної безпеки акторів

Серед множини існуючих СІС для проведення досліджень обрано мережу мікроблогів *Twitter*. Таке рішення обумовлене її високою популярністю, пов'язаною з простотою публікації та швидким пошуком контенту за геш-тегами; використанням в організації масових вуличних протестів під час подій «арабської весни» [10]; доступністю підготовлених баз даних (БД) акаунтів акторів, що забезпечують можливість співставлення отриманих результатів з академічними дослідженнями.

Вхідними даними для проведення експерименту обрано БД акаунтів акторів мікроблогу *Twitter*, отриману в рамках проекту *TheFakeProject* [11], що виконувався групою дослідників *Institute of Informatics and Telematics of the Italian National Research Council* (Італія). Структурно база складається з множини акаунтів реальних користувачів та множини фейкових акаунтів [11] (рис. 1).

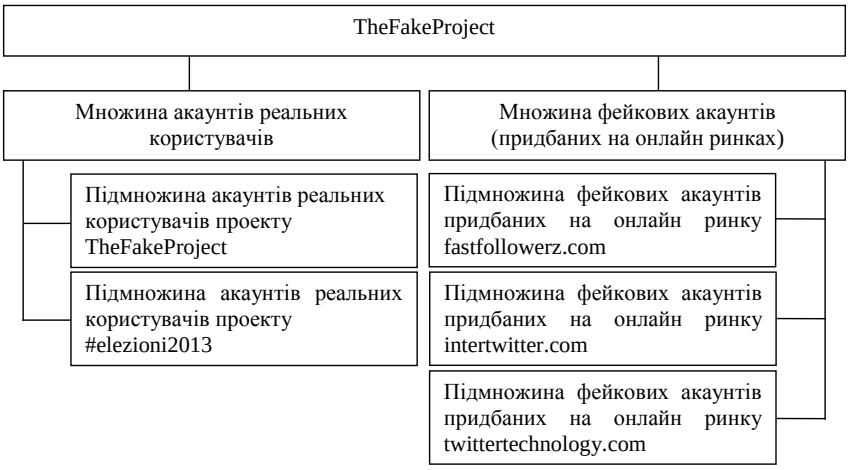

Рисунок 1 – Структура бази даних акторів мережі мікроблогу *Twitter* проекту *TheFakeProject*

Множина профілів реальних акторів створена шляхом агрегації результатів академічних досліджень проектів *TheFakeProject* та *#elezioni2013* (*University of Perugia and Sapienza University of Rome*). Множину фейкових облікових записів сформували придбані на онлайн ринках мережі мікроблогу *Twitter* (http://fastfollowerz.com, http://intertwitter.com, http://twittertechnology.com) 3000 фейкових акаунтів, які зберігаються у відповідній БД. Враховуючи принципові відмінності в концепції функціонування мережі мікроблогу *Twitter* від інших СІС, підхід до побудови профілів інформаційної безпеки акторів адаптовано з урахуванням наступних припущень та обмежень:

БД акаунтів користувачів мережі мікроблогу *Twitter* проекту *TheFakeProject* не є репрезентативною і може бути використана виключно на початковому етапі проектування модуля побудови профілів інформаційної безпеки системи забезпечення інформаційної безпеки держави;

у БД активність публікацій акторами контенту не синхронізована за часом і тематикою, що практично унеможливлює віднесення актора до одного із класів загроз за результатами контент-аналізу повідомлень;

результати попередньої обробки даних не вносять вагомих похибок в результати класифікації.

Експериментальне дослідження методу побудови профілів інформаційної безпеки акторів із врахуванням особливостей функціонування мікроблогу *Twitter*

Для досягнення поставленої мети визначено основні етапи проведення експерименту, які зводяться до такого.

Етап 1. Селекція параметрів сигнатур. Для адекватності проведеного експерименту, при попередній підготовці даних, з БД акаунтів користувачів проекту *TheFakeProject* вилучені малоінформативні та унікальні параметри, які забезпечують однозначну класифікацію підкласів. У табл. 1 представлено атрибути профілів акторів у БД акаунтів, а у третьому стовпчику позначено обрані (+), виключені (-) та використані розрахункові зважені значення атрибутів (*).

Таблиця 1 – Атрибути профілів акторів у БД акаунтів

Категорії профілю інформаційної безпеки актора	Параметр	Обрано/ виключено/ розраховано	Причина виключення
Атрибути профілю актора	id	-	Унікальний
	name	-	Унікальний
	screen_name	-	Унікальний
	statuses_count	+	
	created_at	-	Малоінформативний
	url	-	Малоінформативний
	lang	-	Малоінформативний
	time_zone	-	Малоінформативний
	location	-	Малоінформативний
	default_profile	-	Малоінформативний
	default_profile_image	-	Малоінформативний
	geo_enabled	-	Малоінформативний
	profile_image_url	-	Малоінформативний
	profile_banner_url	-	Малоінформативний
	profile_use_background_image	-	Малоінформативний
	profile_background_image_url_https	-	Малоінформативний
	profile_text_color	-	Малоінформативний
	profile_image_url_https	-	Малоінформативний
	profile_sidebar_border_color	-	Малоінформативний
	profile_background_tile	-	Малоінформативний
	profile_sidebar_fill_color	-	Малоінформативний
	profile_background_image_url	-	Малоінформативний
	profile_background_color	-	Малоінформативний
	profile_link_color	-	Малоінформативний
	utc_offset	-	Малоінформативний
	protected	-	Малоінформативний
	verified	-	Малоінформативний
	description	-	Малоінформативний
	updated	-	Малоінформативний

Активність публікації актором контенту	created_at	-	Малоінформативний
	id	-	Малоінформативний
	text	-	Малоінформативний
	source	-	Малоінформативний
	user_id	-	Малоінформативний
	truncated	-	Малоінформативний
	in_reply_to_status_id	-	Малоінформативний
	in_reply_to_user_id	+	
	in_reply_to_screen_name	-	Малоінформативний
	retweeted_status_id	-	Малоінформативний
	geo	-	Малоінформативний
	place	-	Малоінформативний
	retweet_count	+	
	reply_count	-	Малоінформативний
	favorite_count	-	Малоінформативний
	num_hashtags	*	
	num_urls	*	
	num_mentions	*	
	timestamp	-	Малоінформативний
Лінгвістичні ознаки контенту актора	Публікацій акторами контенту не синхронізована за часом та тематикою публікацій, що робить лінгвістичні ознаки малоінформативними		
Зв'язки актора з учасниками СІС	followers_count	+	
	friends_count	+	
	favourites_count	+	
	listed_count	+	

Етап 2. Формування тестової множини. Аналіз БД проекту *TheFakeProject* показав, що за кількісним співвідношенням фейкових акаунтів і профілів реальних користувачів вона є незбалансованою. Тому на наступному етапі із записів БД методом рандомізації сформовано тестову множину, яка складається з 158 реальних (*real*) і 154 та фейкових (*fake*) акаунтів. Виходячи з результатів проведених досліджень [12] тестова множина сформована таким чином, щоб забезпечити вимогу збалансованості та мінімізувати вплив похибок перенавчання класифікаційних моделей.

Етап 3. Введення метрик оцінювання якості результатів класифікації. Нехай X – множина об'єктів, Y – кінцева множина класів, y^* – рішення щодо належності акторів до одного з класів. Класифікація об'єкта зводиться до відображення $y^* : X \to Y$. Передбачений клас об'єкта, отриманий в результаті відображення y^*, може або співпасти в реальним класом, або ні. Тоді на виході класифікатора можуть бути чотири наступні результати:

TP (*true positives*) – клас 1 вірно класифіковано;

FP (*false positives*) – клас 1 у результаті класифікації помилково віднесено до класу 2;

FN (*false negatives*) – клас 2 помилково класифіковано, як клас 1;

TN (*true negatives*) – клас 2 класифіковано вірно.

При цьому матриця спряженості бінарного класифікатора має вигляд, як подано у табл. 2.

Таблиця 2 – Матриця спряженості бінарного класифікатора

Істинний клас	Результат класифікації	
	Клас 1	Клас 2
Клас 1	TP	FP
Клас 2	FN	TN

З метою оцінювання результатів класифікації введено наступні метрики.

1) Достовірність (*accuracy*) – ступінь збігу результатів відображення з істинними класами

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}.$$

2) Точність (*precision*) показує, яка частка об'єктів від загального числа віднесених до даного класу класифікована вірно

$$\text{Precision} = \frac{TP}{TP + FP}.$$

3) Повнота (*recall*) – метрика, що відображає частку від загального числа об'єктів істинного класу, класифіковану коректно

$$\text{Recall} = \frac{TP}{TP + FN}.$$

4) Для адекватної оцінки результатів класифікації введено метрику, яка об'єднує інформацію про точність і повноту алгоритму, що суперечать один одному – *F*-міру. *F*-міра (*F-measure*) – інтегральний показник, що розраховується як гармонійне середнє між точністю і повнотою

$$F_{measure} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}.$$

5) *MCC* (*Matthew Correlation Coefficient*) – коефіцієнт кореляції, який враховує всі значення матриці спряженості

$$MCC = \frac{TP \cdot TN - FP \cdot FN}{\sqrt{(TP + FN)(TP + FP)(TN + FP)(TN + FN)}}.$$

Етап 4. Експериментальна перевірка припущення про репрезентативність тестової множини. На основі введених метрик виконано перевірку припущення про репрезентативність сформованої тестової множини і виконано оцінювання відповідних похибок (табл. 3). Для цього побудову класифікаційних моделей проведено на основі алгоритмів машинного навчання *Random Forest, J48, Bayesian Network*, а результати класифікації порівнювалися за введеними на етапі 3 метриками.

Таблиця 3 – Похибки алгоритмів машинного навчання

Алгоритм	Множини профілів акторів	Метрики				
		accuracy	*precision*	*recall*	*F-measure*	*MCC*
Random Forest	*TheFakeProject*	0,994	0,997	0,990	0,994	0,987
	Тестова множина	0,994	0,994	0,994	0,994	0,987
	Похибка	0,000	0,003	-0,004	0	0
J48	*TheFakeProject*	0,992	0,991	0,992	0,992	0,983
	Тестова множина	0,987	0,987	0,987	0,987	0,974
	Похибка	0,005	0,004	0,005	0,005	0,009
Bayesian Network	*TheFakeProject*	0,960	0,965	0,954	0,960	0,921
	Тестова множина	0,971	0,972	0,971	0,971	0,943
	Похибка	-0,011	-0,007	-0,017	-0,011	-0,022

Враховуючи порядок формування тестової множини і отримані похибки введених метрик, які в найгіршому випадку не перевищують 0,022, вважатимемо, що сформована множина є репрезентативною відносно генеральної сукупності – БД *TheFakeProject*.

Етап 5. Вибір алгоритмів бінарної класифікації. Для цього виконано побудову класифікаційних моделей на основі наступних алгоритмів: *OneR, NaiveBayes, BayesNet, J48, RandomForest, DecisionTable, JRip, AdaBoost M1 (OneR), AdaBoost M1 (Naive Bayes).* Уніфікацію результатів відбору забезпечено використанням розробленої університетом Уайкато системи аналізу даних *Weka* [13**Ошибка! Источник ссылки не найден.**] і реалізованими в її бібліотеках відповідними алгоритмами машинного навчання. Узагальнюючі здатності алгоритмів оцінювались з використанням процедури емпіричного оцінювання (*cross-validation*) з параметром розбиття 10. Структурна схема послідовності побудови класифікаційних моделей представлена на рис. 2. Отримані оцінки точності класифікації алгоритмів за введеними метриками подані в табл. 4.

За результатами аналізу табл. 4 можна зробити наступні висновки. Відносно прості алгоритми *OneR, NaiveBayes* за умови найвищої швидкодії забезпечують невисокі показники точності, достовірності та повноти класифікації. Найвищі показники за введеними метриками забезпечують алгоритми на базі дерев рішень *J48, RandomForest.* При цьому алгоритм *J48* по відношенню до *RandomForest* має значно вищу швидкодію.

Етап 6. Виділення класів загроз акторів. Тестову множину було поділено на наступні класи: реальний активний актор (*active_real*), реальний пасивний актор (*passive_real*), фейковий активний актор (*active_fake*), фейковий пасивний актор (*passive_fake*). Поділ на такі класи ґрунтується на припущенні про універсальність закону Меткалфа [14] і можливість його застосування не тільки для інформаційно-телекомунікаційних мереж, а й СІС як мереж соціальних взаємозв'язків акторів. Виходячи з такого при-

пущення, корисність актора як суб'єкта інформаційної операції пропорційна квадрату кількості його друзів.

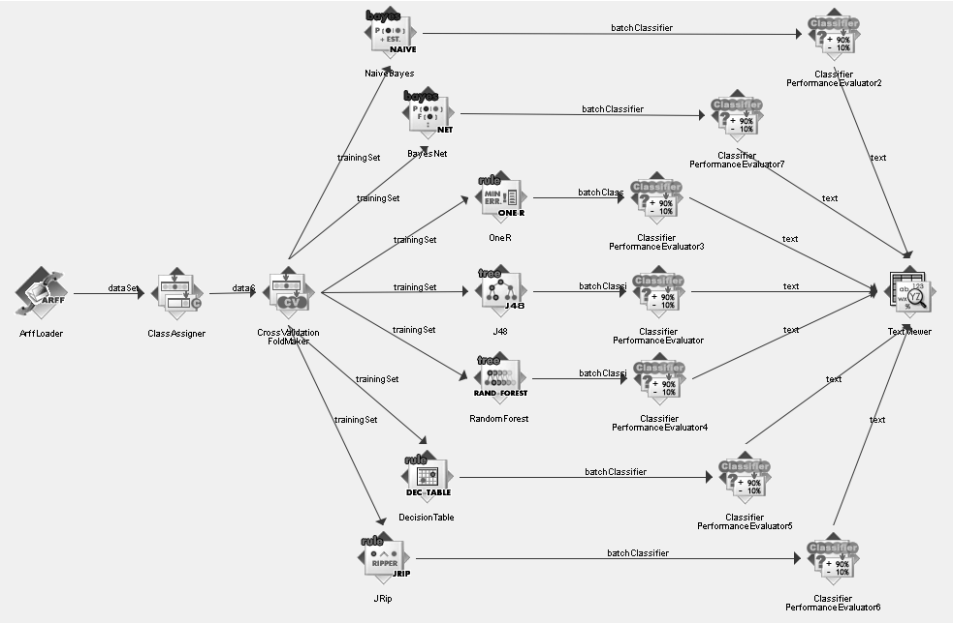

Рисунок 2 – Структурна схема послідовності побудови класифікаційних моделей у системі аналізу даних *Weka*

Таблиця 4 – Оцінки точності класифікації

Алгоритм	Час побудови класифікаційної моделі	*accurancy*	*precision*	*recall*	*F-measure*	*MCC*	
OneR	0,01	0,949	0,932	0,949	0,94	0,878	real_users
		0,929	0,947	0,929	0,938	0,878	fake_users
		0,939	0,939	0,939	0,939	0,878	Weighted Avg
NaiveBayes	0,02	0,975	0,981	0,975	0,978	0,955	real_users
		0,981	0,974	0,981	0,977	0,955	fake_users
		0,978	0,978	0,978	0,978	0,955	Weighted Avg
BayesNet	0,06	0,994	0,952	0,994	0,972	0,943	real_users
		0,948	0,993	0,948	0,970	0,943	fake_users
		0,971	0,972	0,971	0,971	0,943	Weighted Avg
J48	0,02	0,987	0,987	0,987	0,987	0,974	real_users
		0,987	0,987	0,987	0,987	0,974	fake_users
		0,987	0,987	0,987	0,987	0,974	Weighted Avg
RandomForest	0,07	0,994	0,994	0,994	0,994	0,987	real_users
		0,994	0,994	0,994	0,994	0,987	fake_users
		0,994	0,994	0,994	0,994	0,987	Weighted Avg
DecisionTable	0,16	0,981	0,957	0,981	0,969	0,936	real_users
		0,955	0,98	0,955	0,967	0,936	fake_users
		0,968	0,968	0,968	0,968	0,936	Weighted Avg
JRip	0,06	0,987	0,994	0,987	0,99	0,981	real_users
		0,994	0,987	0,994	0,99	0,981	fake_users
		0,99	0,99	0,99	0,99	0,981	Weighted Avg
AdaBoost M1 (Naive Bayes)	0,06	0,975	0,994	0,975	0,984	0,968	real_users
		0,994	0,975	0,994	0,984	0,968	fake_users
		0,984	0,984	0,984	0,984	0,968	Weighted Avg
AdaBoost M1 (OneR)	0,05	0,968	0,975	0,968	0,971	0,942	real_users
		0,974	0,968	0,974	0,971	0,942	fake_users
		0,971	0,971	0,971	0,971	0,942	Weighted Avg

Такий ефект пояснюється зростанням швидкості поширення контенту актором зі збільшенням кількості його друзів і, як наслідок, зацікавленості суб'єктів інформаційних операцій до його залучення. Таких акторів віднесено до класу активних потенційних загроз *(active_real),* у протилежному випадку – до класу *passive_real.* Аналогічний поділ виконано і для фейкових акаунтів акторів.

Етап 7. Оцінювання точності класифікації різними алгоритмами. Для більш детального аналізу результатів класифікації профілів акторів обрано три алгоритми класифікації з тих, які забезпечили досягнення найвищих значень введених метрик оцінювання – *J48, RandomForest, JRip*. Отримані в результаті побудови класифікаційних моделей значення метрик оцінювання для обраних алгоритмів машинного навчання подані в табл. 5.

Таблиця 5 – Метрики оцінювання алгоритмів за класами

Істинний клас	Алгоритм	*accurancy*	*precision*	*recall*	*F-measure*	*MCC*
PASSIVE_FAKE	J48	0,972	0,972	0,972	0,972	0,958
	RandomForest	0,991	0,982	0,991	0,986	0,979
	JRip	0,963	0,963	0,963	0,963	0,944
ACTIVE_FAKE	J48	1	0,957	1	0,978	0,975
	RandomForest	1	0,978	1	0,989	0,987
	JRip	0,956	0,956	0,956	0,956	0,948
PASSIVE_REAL	J48	0,976	0,984	0,976	0,980	0,967
	RandomForest	0,984	1	0,984	0,992	0,987
	JRip	0,976	0,969	0,976	0,973	0,954
ACTIVE_REAL	J48	0,968	1	0,968	0,984	0,982
	RandomForest	1	1	1	1	1
	JRip	0,935	0,967	0,935	0,951	0,946

З табл. 5 видно, що обраними алгоритмами найбільш повно класифікується клас *active_real*, найгірше – *passive_fake*. Клас *active _fake* більш точно визначають алгоритми *J48* і *JRip*, а клас *passive_real* – алгоритми *RandomForest* та *JRip*. При цьому загальну найвищу точність розподілу за класами забезпечує алгоритм *RandomForest.* Отримані результати збіжні з результатами академічних досліджень [15, 16] і задовольняють вимогам швидкодії, які висуваються до підсистем виявлення загроз у СІС. Вибір конкретного методу класифікації для побудови профілів інформаційної безпеки акторів доцільно робити залежно від специфіки інформаційної операції у СІС і вимог до точності та швидкодії підсистеми виявлення ознак загроз.

Висновки

1. Експериментально доведено дієвість запропонованого методу побудови профілів інформаційної безпеки акторів СІС для вирішення проблеми завчасного виявлення ознак загроз інформаційній безпеці держави. Розроблений підхід може бути адаптовано для застосування у різних видах СІС з метою врахування особливостей їх функціонування.

2. Встановлено, що вибір методу класифікації виконується відповідно до вимог точності та швидкодії окремих складових системи забезпечення інформаційної безпеки держави у СІС. Використання підходу до побудови профілів інформаційної безпеки акторів у СІС підвищить загальну ефективність функціонування системи інформаційної безпеки держави у СІС, що є актуальною проблемою для України.

Список літератури

1. Analysis of topological characteristics of huge online social networking services / Y.-Y. Ahn, S. Han, H. Kwak, S. Moon, H. Jeong // Proceedings of the 16th international conference on World Wide Web. – ACM, NewYork, 2007. – PP. 835–844.

2. Keenan A. Sociability and social interaction on social networking websites / A. Keenan, A. Shiri // LibraryReview. – Vol. 58, Iss. 6. – PP. 438–450.

3. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; під заг. ред. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

4. Молодецька К. В. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах / К. В. Молодецька // Защита информации : сб. науч. труд. – 2016. – Вып. 23. – С. 75–87.

5. Определение демографических атрибутов пользователей микроблогов / А. Коршунов, И. Белобородов, А. Гомзин [и др.] // Труды Института системного программирования РАН. – 2013. – Т. 25. – С. 179–194.

6. Гомзин А. Г. Методы построения социо-демографических профилей пользователей сети Интернет / А. Г. Гомзин, С. Д. Кузнецов // Труды Института системного программирования РАН. – 2015. – Т. 27. – Вып. 4. – С. 129–143.

7. Pennacchiotti M. Democrats, republicans and Starbucks afficionados: user classification in Twitter / M. Pennacchiotti, A. M. Popescu // Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and datamining. – ACM, 2011. – С. 430–438.

8. Beller C. I'm a Belieber: Social Roles via Self-identification and Conceptual Attributes / C. Belleretal // Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics. – 2014. – PP. 181–186.

9. Молодецька-Гринчук К. В. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2017. – № 2(26). – С. 104–110.

10. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К. : Інтертехнологія, 2009. – 164 с.

11. MIB Datasets : [Online resource] / MIB Datasets. – Access mode : http://mib.projects.iit.cnr.it/dataset.html. – Title from the screen.

12. Weiss G. M. Learning when training data are costly: the effect of class distribution on tree induction / G. M. Weiss, F. Provost // Journal of Artificial Intelligence Research. – 2003. – 19. – PP. 315–354.

13. Weka 3 – Data Mining with Open Source Machine Learning Software in Java / Weka. – Access mode : http://www.cs.waikato.ac.nz/ml/weka/. – Title from the screen.

14. Меткалф Б. Закон Меткалфа сорок лет спустя после рождения Ethernet / Б. Меткалф // Открытые системы. СУБД. – 2014. – № 1. – С. 44–47.

15. Cresci S. Fame for sale: Efficient detection of fake Twitter followers / S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, M. Tesconi // Decision Support Systems. – 2015. – Vol. 80. – PP. 56–71.

16. Jensen U. Random Forest classification of Twitter users to detect features linked to bot susceptibility / U. Jensen, Chr. Schenk // Professional profile of Ulf Aslak. – Access mode : http://ulfaslak.com/portfolio/sigproc-sp.pdf. – Title from the screen.

Стаття надійшла: 25.08.2017.

Відомості про авторів

Грищук Руслан Валентинович – д.т.н., старший науковий співробітник, начальник науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова.

Мамарєв Віктор Миколайович – к.т.н., провідний інженер відділу науково-дослідної та випробувальної роботи Національного центру управління та випробувань космічних засобів, вул. Московська, 8.

Молодецька-Гринчук Катерина Валеріївна – к.т.н., доцент, доцент кафедри комп'ютерних технологій і моделювання систем, Житомирський національний агроекологічний університет, бульвар Старий, 7.