ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

UDC 004.9

DOI: https://doi.org/10.30837/ITSSI.2020.13.052

YE. MELESHKO

THE METHOD OF DETECTING INFORMATION ATTACK OBJECTS IN RECOMMENDATION SYSTEM BASED ON THE ANALYSIS OF RATING TRENDS

The **subject** matter of the research is the process of identifying information attacks on the recommendation system. The **goal** of this work is to develop a method for detecting information attack objects in a recommendation system based on the analysis of trends in the ratings of system objects. The **task** to be solved is: develop a method of detecting information attack objects in a recommendation system. **Results.** The paper investigates methods for determining the existing trends in time series, in particular, methods based on a moving average, several moving averages and zigzag tops. Also, a method for predicting the dynamics of trends in a time series in the future based on R/S analysis was considered. The set of indicators has been proposed, by the values of which it is possible to determine the presence or absence of an information attack on an object of the recommendation system. This set of indicators includes: the existing trend in the numerical series of ratings of the system object, the predicted trend in the ratings of the system object, the number of getting of the object in the lists of recommendations and statistical characteristics of the series, for example, the number of target ratings, the variance of ratings, the variance of the time of assigning ratings, etc. On the basis of the proposed set of indicators, the method for detecting objects of information attack in a recommendation system using trend analysis in the ratings of system objects was developed. This method makes it possible to detect the presence of an information attack on the objects of the recommender system and generates the list of possible targets for bots. Many possible targets can be used to further search for bot profiles and clarify information about their true targets. This will make it possible, when searching for botnets, to check not all system profiles, but only those that interacted with probable targets of attack. **Conclusions.** The method of detecting information attack objects in recommendation system based on the analysis of rating trends was developed. The software implementation was created and experiments to test the effectiveness of the developed method were carried out. The experiments have shown that the developed method makes it possible to identify with high accuracy the objects of information attacks on recommender systems for random, average and popular attack models.

Keywords: recommendation systems; information attacks; information security; information attack detection; technical analysis; moving average; R/S analysis.

Introduction

Recommendation systems are increasingly used on various websites and are becoming an important part of them, allowing users to better find the content they need [1, 2].

Like other components of multi-user websites, referral systems need to be protected from information attacks that may be used to disseminate informational influences for marketing, political or other purposes [3, 4].

The main type of information attacks on referral systems are profile injection attacks [3-7]. They are implemented by bot networks [4, 5]. Such attacks are aimed at changing the frequency of impressions in the recommendations of certain objects of the system. Increasing the frequency of impressions in the recommendations draws more attention to certain content. And reducing the frequency of impressions - reduces the likelihood of users' attention to the content. Therefore, attacks on referral systems are used by attackers to draw attention to their content, or to reduce the popularity of competitors' content. There are different models of profile injection attacks, in particular, random, medium and popular attack models [6, 7], which differ in strategies for filling bot profiles with estimates for targets and for filling the profile and masking it as a user profile from the target system segment.

Existing methods of detection and neutralization of attacks in recommendation systems [1, 8-11], require constant repeated checks of all profiles of system users.

Mostly in existing studies, it is proposed to consider the detection of an attack on the recommendation system identical to the detection of bot profiles [1, 4, 8-11]. To identify bot profiles, clustering and classification methods are used to separate all system profiles into normal and suspicious, and the distribution of ratings in individual user profiles is analyzed by statistical methods to find anomalies specific to bot profiles.

Detecting bot profiles is a very resource-intensive task that requires the use of machine learning methods and processing large amounts of data.

In this paper, it is proposed to identify the objects of information attack in the recommendation system, and then, if such are found, you can further search for bot profiles among users who interacted with them. It is suggested to look for objects of attack on the basis of statistical characteristics and dynamics of trends of their ratings. In this case, detecting the presence of an attack will be a less resource-intensive task, and bots can be searched among fewer user profiles.

Main part

We will assume that the attack on the recommendation system occurs when the dynamics of ratings of one or more objects of the system changes as a result of the actions of the bot network. However, the amount of damage from an attack does not always depend on the number of objects affected. Successful change of ratings of even one object by a botnet can have big consequences if it is a question, for example, of social, political or medical sphere, etc.

Thus, the presence of an information attack on the recommendation system causes a change in the ratings of objects (increases or decreases them), but a change in the ratings of the object is not sufficient reason to believe that an attack occurs, as ratings may change as a result of normal actions of authentic users. Therefore, we highlight a number of additional features that may indicate an information attack:

- in the case of an object, the number of ratings has increased sharply over the period of study – this may indicate an attack, because to shift the ratings you need to create a significant number of bots that will deliver targeted ratings of the object;
- object, on the studied period of time put a lot of target ratings, i.e., the highest when increasing the rating, or the lowest when lowering the rating - such ratings may be higher than all others in the current period, which may indicate the haste of the attacking system when he needs to promote his content as soon as possible;
- low variance of object ratings - it is natural that the attack object will have many identical marks in the studied period of time, because during the attack they try to change ratings, i.e., for example, before the attack there were many low marks, and the botnet exposes many high estimates;
- the object became more often than others to get on the recommendation lists – if it is an attack, it is successful, in fact only successful attacks and should be of interest to the security subsystem of the recommendation system, because they must be neutralized, and unsuccessful attacks can be ignored in case of savings system resources.

So, let's form a set of indicators, the values of which can determine the presence or absence of an information attack on the object of the recommendation system:

$$Q_{a,i} = \{tr, pr, d_r, d_t, n_r, n_{tr}, n_{rec}\}, \qquad (1)$$

where *tr* is a trend of dynamics of object i ratings, which can take the following values {–1, 0, 1} – respectively "rating downward trend", "no change" and "upward trend"; *pr* – forecasting the trend of the dynamics of object i ratings; d_r – variance of object i ratings; d_t – variance of object i rating time; n_r – the number of estimates in the object i and in the studied period of time; n_{tr} – the number of target estimates in the object i in the studied period of time; n_{rec} – the number of hits of the object i and the lists of recommendations to users in the study period.

If the objects of the system can be ranked according to their importance in terms of the need for protection against attacks, they can be assigned the appropriate coefficients and primarily monitor the status and dynamics of ratings of the most important objects, ignoring, or lastly monitoring the status of ratings less important objects.

Of all the indicators (1), it is difficult to determine only trends and forecasts of trend dynamics. Since the definition of trends is the economic science, for example, to determine changes in exchange rates, stocks, etc., we turn to their tools, namely to technical analysis [12, 13].

Technical analysis is a set of tools used in the economy to predict future price changes based on the analysis of patterns of price changes in the past.

In technical analysis, there are many methods for determining the direction of the trend [12-15], consider the simplest of them, which can be easily applied not only to prices in trading systems, but also to any time series:

- moving average;
- for several moving averages;
- behind the vertices of the zigzag.

Determining the direction of the trend on the moving average.

One of the easiest ways to determine the presence of a trend and its direction - the moving average. You can use both a single moving average and a whole set, which is sometimes called a "fan".

The rule for determining the trend for one moving average:

- the trend is directed upwards, if at a given period of time the last value of the numerical series is above the moving average;
- the trend is directed downwards, if at a given period of time the last value of the numerical series is below the moving average.

When at a given time the last value of the numerical series is above / below the moving average, the next value often then unfolds in the opposite direction. That is, this method gives a large number of incorrect answers. Due to this, its use as a trend indicator is quite limited. It can only be used as the coarsest trend filter.

Determining the direction of the trend by several moving averages.

To improve the quality of the moving trend, you can, for example, use two or more moving averages with different periods. Then the rule for determining the trend for any number (more than one) of moving averages with different periods will look like this:

- the trend is directed upwards, if at a given period of time all moving averages are built in the correct order of increase to the end of the numerical series;
- the trend is directed downwards, if at a given period of time all moving averages are built in the correct order of decrease to the end of the numerical series.

In this method, the number of false signals about the change in the direction of the trend will be less than in the previous one. But the time spent on determining the trend will increase.

Determining the direction of the trend by the highs and lows of the ZigZag indicator.

This method uses the rule of Charles Doe [12]:

- the trend is directed upwards, if each subsequent local maximum of the graph of the numerical series is higher than the previous local maximum and, at the same time, each subsequent local minimum of the graph of the numerical series is also higher than the previous local minimum;
- the trend is directed downwards, if each subsequent local minimum of the graph of the numerical series is below the previous local minimum and, at the same time, each subsequent local maximum of the graph of the

numerical series is also below the previous local maximum.

Local highs / lows can be found behind the vertices of the ZigZag indicator.

The ZigZag indicator is a trend indicator in technical analysis that connects local lows and highs on a numerical series graph and allows you to filter noise. There are many different modifications of the ZigZag indicator for stock market analysis.

The minimum time series value change parameter determines the number of points to which the value must move to form a new Zig or Zag line. Thus, the ZigZag reflects only the most significant changes and reversals.

The main disadvantage of this method of determining the trend - in real time it is impossible to understand the already formed extremum or not.

This disadvantage makes this method of little value for practical use in real time. But it is very useful in the technical analysis of previously collected data in order to find patterns and to assess the quality of the system.

In addition to identifying the current trend, you can also try to predict possible further changes in the time series. In the context of determining the presence of an attack on a recommendation system, predicting the preservation of an abnormal trend can be an additional indicator of a successful attack.

R/S analysis can be used to predict future trends in numerical series [15].

Consider the algorithm of R/S analysis. It consists of the following steps:

1. Given the initial time series St. Let’s calculate the logarithmic ratio:

$$N_t = \ln \frac{S_t}{S_{t-1}} . \qquad (2)$$

2. Let’s divide the series N by A adjacent periods of length n. Let’s denote each period as Ia, where $a = 1, 2, \ldots, A$. Determine for each Ia the average value:

$$E(I_a) = \frac{1}{n}\sum_{k=1}^{n} N_{k,a} . \qquad (3)$$

3. Let’s calculate the deviation from the mean for each period I_a:

$$X_{k,a} = \sum_{i=1}^{k}\left(N_{i,a} - E(I_a)\right). \qquad (4)$$

4. Let’s calculate the scope within each period:

$$R_{I_a} = \max\left(X_{k,a}\right) - \min\left(X_{k,a}\right). \qquad (5)$$

5. Let’s calculate the standard deviation for each period I_a:

$$S_{I_a} = \sqrt{\frac{1}{n}\sum_{k=1}^{n}\left(N_{k,a} - E(I_a)\right)^2} . \qquad (6)$$

6. Each R_{I_a} we divide by S_{I_a}. Next, we calculate the average value *R/S*:

$$R/S(n) = \frac{\sum_{a=1}^{A} R/S(A)}{A} . \qquad (7)$$

7. Increase n and repeat steps 2-6 until $n \le N/2$.

8. Build a graph of dependence $\log\left(R/S(n)\right)$ from $\log(n)$ and using the least squares method we find the regression of the form:

$$\log\left(R/S(n)\right) = H \cdot \log(n) + c , \qquad (8)$$

where *H* is a Hirst index.

9. Next, let’s check the result for significance. To do this, we test the hypothesis that the analyzed structure is normally distributed. If *R/S* are random variables normally distributed, then we can assume that *H* is also normally distributed. The asymptotic limit for the independent process is the Hirst index equal to 0.5. Peters [15], as well as Ennis and Lloyd [16] suggested to use the following expected *R/S*:

$$E\left(R/S(n)\right) = \frac{n-0.5}{n} \cdot \left(n \cdot \frac{\pi}{2}\right)^{-0.5} \cdot \sum_{r=1}^{n-r} \sqrt{\frac{n-r}{n}} . \qquad (9)$$

For *n* observations we find the expected Hirst index *E(H).*

10. Let’s calculate the expected variance of the Hirst index by the formula:

$$Variance(H) = \frac{1}{N} . \qquad (10)$$

where *H* – is the Hirst index; N – the number of observations in the sample.

11. Let’s check the significance of the obtained Hirst coefficient by estimating the number of standard deviations by which *H* exceeds *E(H).* The result is considered significant when the significance indicator on the module is more than 2.

Interpretation of Hearst index indicators:

– $H = 0.5$ – process with no memory, no trend.

– $H > 0.5$ – the process tends to maintain the trend.

– $H < 0.5$ – the process is characterized by antipersensitivity, i.e. any tendency tends to change to the opposite.

The values of the Hirst index of natural processes are grouped near the values of 0.72–0.73, which is indicated in the following works [17].

When studying the state of the recommendation system, it makes sense to pay attention to objects in which *H*> 0.5 in the studied period of time, such objects will change their ratings according to a certain trend over a long period of time, therefore, among them may be goals of successful information attacks, especially if *H*> 0.73.

A method of detecting objects of information attack has been developed, which consists of the following stages:

Stage 1. We form a set of objects *I* for checking, it can contain all objects of system, or only critically important objects which need protection against attacks.

Stage 2. Determine with the help of several moving averages (or other methods of trend determination) for each object from the set *I* the indicator *tr* over time *τ*.

Stage 3. Determine by *R/S* analysis for each object from the set *I* Hearst index *H* over time *τ*.

Stage 4. Determine for each object from the set *I* on the time interval *τ* the variance of the estimates d_r and the variance of the time intervals between the setting of the target estimates d_t , as well as their average values in the systems $d_{\tau,av}$ та $d_{t,av}$.

Stage 5. Determine for each object from the set *I* time interval *τ* the number of target n_{tg} and all estimates n_r , as well as the average number of target $n_{tg,av}$ and all estimates $n_{r,av}$ for system objects.

Stage 6. Determine for each object from the set *I* time interval *τ* the number of hits in the lists of recommendations n_{rec} , as well as the average number of hits in the lists of recommendations $n_{rec,av}$ for all objects of the system.

Stage 7. Determine the presence and type of attack according to the following rules:

Rule 1. If the object has any 5 signs from the data: the trend of rising ratings $tr_\tau = 1$, $H > 0.73$, $d_\tau \le d_{\tau,av}$, $d_t \le d_{t,av}$, $n_r > n_{r,av}$, $n_{tg} > n_{tg,av}$, $n_{rec} > n_{rec,av}$, then we believe that there is a high probability of an attack to increase the rating for this object.

Rule 2. If the object has any 5 characteristics from the data: the trend of decreasing rating: $tr_\tau = -1$, $H > 0.73$, $d_\tau \le d_{\tau,av}$, $d_t \le d_{t,av}$, $n_r > n_{r,av}$, $n_{tg} > n_{tg,av}$, $n_{rec} < n_{rec,av}$, we believe that there is a high probability of a downgrade attack for this object.

To test the developed method, software in the Python programming language using the Neo4j database will be implemented. The open data set MovieLens Datasets was used as input data, the data of the simulated information attacks on the recommendation system was added to it. Attacks were modeled using the models of information attacks given in [1, 6, 7].

A series of experiments was performed to test the effectiveness of the proposed method. The results of the experiments are shown in table1.

Table 1. *The results of testing the developed method of detecting information attack by injecting profiles on the recommendation system and objects of attack*

No. of experiment	Model of information attack by injection of profiles	Number of objects in the system	Number of bot attack objects	Correctly recognized objects of attack, %	Falsely recognized as objects of attack, %	RMSE
1	Random attack	200	20	100.00	5.55	0.223
2		200	10	80.00	23.68	0.484
3		200	5	40.00	22.05	0.479
4		200	1	100.00	16.58	0.406
5	Medium attack	200	20	90.00	0.00	0.100
6		200	10	50.00	13.68	0.393
7		200	5	60.00	13.84	0.380
8		200	1	100.00	12.06	0.346
9	Popular attack	200	20	75.00	0.00	0.158
10		200	10	80.00	12.63	0.360
11		200	5	40.00	17.94	0.435
12		200	1	100.00	15.57	0.393
Average values:				76.25	12.79	0.346

According to the results of experiments, the developed method allows to detect on average 76% of objects of information attacks in the recommendation system. Objects that were not attacked by information and were mistakenly identified as being attacked accounted for an average of 13%.

From objects that have signs of information attack on them, you can form a set Ig. This will allow the search for botnets to check not all system profiles, but only those that interacted with the objects of the Ig set. After finding the bot network, you can refine the data based on the analysis of the activity of bots obtained by the developed method.

Conclusions

The study of methods for determining existing trends in time series, in particular, methods based on moving averages, several moving averages and ZigZag vertices has been done. Also, the method of forecasting the dynamics of time series trends in the future based on R/S analysis is considered.

There are many indicators that can be used to determine the presence or absence of an information attack on the object of the recommendation system. This set of indicators includes the current trend of system object ratings, the forecast trend of system object ratings, the number of object hits in the recommendation lists and statistical characteristics of the series, such as the number of target estimates, variance of estimates, etc.

Based on the proposed set of indicators, a method for identifying objects of information attack in the recommendation system using trend analysis in the ratings of system objects has been developed.

The developed method allows to detect the presence of an information attack on the objects of the recommendation system, as well as forms a set of probable targets of bots. Many probable targets can be used to further search for bot profiles and refine information about their actual targets. This will allow the search for botnets to check not all system profiles, but only those that interacted with the probable targets of the attack.

The developed method was implemented and experiments were conducted to test its effectiveness. The conducted experiments showed that the developed method allows to detect with high accuracy the objects of information attacks on recommendation systems in random, medium and popular attack models.

References

1. Editors Ricci, F., Rokach, L., Shapira, B., Kantor, P. B. (2010), *Recommender Systems Handbook*, 1st edition, New York, NY, USA : Springer-Verlag New York, Inc., 842 p. DOI: https://doi.org/10.1007/978-0-387-85820-3

2. Valois, B. Jr. C., Oliveira, M. A. (2011), "Recommender systems in social networks", *JISTEM J.Inf.Syst. Technol. Manag.*, Vol. 8 No. 3, P. 681–716, available at : https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752011000300009

3. Lam, S. K., Riedl, J. (2004), "Shilling recommender systems for fun and profit", *Proceedings of the 13th International World Wide Web Conference*, P. 393–402.

4. O'Mahony, M. P., Hurley, N. J., Silvestre G. C. M. (2002), "Promoting recommendations: An attack on collaborative filtering", *From book Database and Expert Systems Applications: 13th International Conference*, DEXA Aix-en-Provence, France, P. 494–503, available at : https://link.springer.com/chapter/10.1007/3-540-46146-9_49

5. Kumari, T., Punam, B. (2017), "A Comprehensive Study of Shilling Attacks in Recommender Systems", *IJCSI International Journal of Computer Science Issues*, Vol. 14, Issue 4, available at : https://www.ijcsi.org/papers/IJCSI-14-4-44-50.pdf

6. Kaur, P., Goel, S., (2016), "Shilling attack models in recommender system", *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, P. 1–5. DOI: 10.1109/INVENTIVE.2016.7824865

7. Gunes, I., Kaleli, C., Bilge, A., et al. (2014), "Shilling attacks against recommender systems: a comprehensive survey", *Artif Intell Rev*, No. 42, P. 767–799. DOI: https://doi.org/10.1007/s10462-012-9364-9

8. Zhou, W., Wen, J., Qu, Q., Zeng, J., Cheng, T. (2018), "Shilling attack detection for recommender systems based on credibility of group users and rating time series", *PLoS ONE*, No. 13 (5): e0196533, available at : https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0196533

9. Chirita, P. A., Nejdl, W., Zamfir, C. (2005), "Preventing shilling attacks in online recommender systems", *In Proceedings of the ACM Workshop on Web Information and Data Management*, P. 67–74, available at : https://dl.acm.org/doi/10.1145/1097047.1097061

10. Zhou, W., Wen, J., Koh, Y. S., Alam, S., Dobbie, G. (2014), "Attack detection in recommender systems based on target item analysis", *2014 International Joint Conference on Neural Networks (IJCNN)*, Beijing, P. 332–339, available at : https://ieeexplore.ieee.org/document/6889419

11. Williams, C. A., Mobasher, B., Burke, R. (2007), "Defending recommender systems: detection of profile injection attacks, *Service Oriented Computing and Applications*, P. 157–170.

12. Murphy, J. J. (2011), *Technical Analysis of the Futures Markets: A Comprehensive Guide to Trading Methods and Applications*, Moscow : Alpina Publisher, 610 p.

13. Schwager, J. (2017), *Technical Analysis. Complete course*, Moscow : Alpina Publisher, 804 p.

14. Prechter, R., Frost A. (2012), *Elliot Wave Principle: Key to Stock Market Profits*, Moscow : Alpina Publisher, 269 p.

15. Peters, E. (2004), *Fractal Market Analysis: Applying Chaos Theory to Investment and Economics*, Moscow : Internet-Trading, 304 p.

16. Anis, A. A., Lloyd, E. H. (1976), "The expected value of the adjusted rescaled Hurst range of independent normal summands", *Biometrica*, No. 63, P. 283–298.

17. Kalush, Ju. A., Loginov, V. M. (2002), "Hurst exponent and its hidden properties", *Siberian Journal of Industrial Mathematics*, Vol. 5, No. 4, P. 29–37.

Received 25.08.2020

Відомості про авторів / Сведения об авторах / About the Authors

Мелешко Єлизавета Владиславівна – кандидат технічних наук, доцент, Центральноукраїнський національний технічний університет, доцент кафедри кібербезпеки та програмного забезпечення, Кропивницький, Україна; email: elismeleshko@gmail.com; ORCID: https://orcid.org/0000-0001-8791-0063.

Мелешко Елизавета Владиславовна – кандидат технических наук, доцент, Центральноукраинский национальный технический университет, доцент кафедры кибербезопасности и программного обеспечения, Кропивницкий, Украина.

Meleshko Yelyzaveta – PhD (Engineering Sciences), Associate Professor, Central Ukrainian National Technical University, Associate Professor of the Department of Cybersecurity and Software, Kropyvnytskyi, Ukraine.

МЕТОД ВИЯВЛЕННЯ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ АТАКИ У РЕКОМЕНДАЦІЙНІЙ СИСТЕМІ НА ОСНОВІ АНАЛІЗУ ТРЕНДІВ РЕЙТИНГІВ

Предметом дослідження є процес виявлення інформаційних атак на рекомендаційну систему. **Метою** даної роботи є розробка методу виявлення об'єктів інформаційної атаки у рекомендаційній системі на основі аналізу трендів у рейтингах об'єктів системи. **Задача**: розробити метод виявлення об'єктів інформаційної атаки у рекомендаційній системі. **Результати.**

У роботі проведено дослідження методів визначення наявних трендів у часових рядах, зокрема, методів на основі ковзного середнього, декількох ковзних середніх та вершин зигзагу. А також розглянуто метод прогнозування динаміки трендів часового ряду у майбутньому на основі R/S-аналізу. Запропоновано множину показників, по значенням яких можна визначити наявність чи відсутність інформаційної атаки на об’єкт рекомендаційної системи. У дану множину показників увійшли: наявний тренд числового ряду рейтингів об’єкту системи, прогнозований тренд рейтингів об’єкту системи, велика кількість потраплянь об’єкту у списки рекомендацій та статистичні характеристики ряду, наприклад, кількість цільових оцінок, дисперсія оцінок, дисперсія часу виставлення оцінок, тощо. На основі запропонованої множини показників розроблено метод виявлення об’єктів інформаційної атаки у рекомендаційній системі з використанням аналізу трендів у рейтингах об’єктів системи. Даний метод дозволяє виявити наявність інформаційної атаки на об’єкти рекомендаційної системи та формує список ймовірних цілей ботів. Множину ймовірних цілей можна використати для подальшого пошуку профілів ботів та уточнення інформації про їх дійсні цілі. Це дозволить при пошуку бот-мереж перевіряти не всі профілі системи, а тільки ті, які взаємодіяли з ймовірними об’єктами атаки. **Висновки**. Розроблено метод виявлення об’єктів інформаційної атаки у рекомендаційній системі на основі аналізу трендів рейтингів. Створено програмну реалізацію та проведено експерименти для перевірки ефективності розробленого методу. Проведені експерименти показали, що запропонований метод дозволяє з високою точністю виявляти об’єкти інформаційних атак на рекомендаційні системи при випадкових, середніх та популярних моделях атак.

Ключові слова: рекомендаційні системи; інформаційні атаки; інформаційна безпека; виявлення інформаційної атаки; технічний аналіз; ковзне середнє; R/S-аналіз.

МЕТОД ОБНАРУЖЕНИЯ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ АТАКИ В РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЕ НА ОСНОВЕ АНАЛИЗА ТРЕНДОВ РЕЙТИНГОВ

Предметом исследования является процесс выявления информационных атак на рекомендательную систему. **Целью** данной работы является разработка метода обнаружения объектов информационной атаки в рекомендательной системе на основе анализа трендов в рейтингах объектов системы. **Задача**: разработать метод выявления объектов информационной атаки в рекомендательной системе. **Результаты**. В работе проведено исследование методов определения имеющихся трендов во временных рядах, в частности, методов на основе скользящего среднего, нескольких скользящих средних и вершин зигзага. А также рассмотрен метод прогнозирования динамики трендов временного ряда в будущем на основе R/S-анализа. Предложено множество показателей, по значениям которых можно определить наличие или отсутствие информационной атаки на объект рекомендательной системы. В данное множество показателей вошли: имеющийся тренд числового ряда рейтингов объекта системы, прогнозируемый тренд рейтингов объекта системы, количество попаданий объекта в списки рекомендаций и статистические характеристики ряда, например, количество целевых оценок, дисперсия оценок, дисперсия времени выставления оценок и т.д. На основе предложенного множества показателей разработан метод обнаружения объектов информационной атаки в рекомендательной системе с использованием анализа трендов в рейтингах объектов системы. Данный метод позволяет выявить наличие информационной атаки на объекты рекомендательной системы и формирует список возможных целей ботов. Множество возможных целей можно использовать для дальнейшего поиска профилей ботов и уточнения информации об их истинных целях. Это позволит при поиске бот-сетей проверять не все профили системы, а только те, которые взаимодействовали с вероятными объектами атаки. **Выводы**. Разработан метод выявления объектов информационной атаки в рекомендательной системе на основе анализа трендов рейтингов. Создана программная реализация и проведены эксперименты для проверки эффективности разработанного метода. Проведенные эксперименты показали, что разработанный метод позволяет с высокой точностью выявлять объекты информационных атак на рекомендательные системы при случайных, средних и популярных моделях атак.

Ключевые слова: рекомендательные системы; информационные атаки; информационная безопасность; выявление информационной атаки; технический анализ; скользящее среднее; R/S-анализ.

Бібліографічні описи / Bibliographic descriptions

Мелешко Є. В. Метод виявлення об’єктів інформаційної атаки у рекомендаційній системі на основі аналізу трендів рейтингів. *Сучасний стан наукових досліджень та технологій в промисловості*. 2020. № 3 (13). С. 52–57. DOI: https://doi.org/10.30837/ITSSI.2020.13.052.

Meleshko, Ye. (2020), "The method of detecting information attack objects in recommendation system based on the analysis of rating trends", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (13), P. 52–57. DOI: https://doi.org/10.30837/ITSSI.2020.13.052.