The recommendation systems used to form a news feed in social networks or to create recommendation lists on content websites or Internet stores are often exposed to information profile injection attacks. These attacks are aimed at changing ratings, and thus at changing the frequency of appearing in recommendations, certain objects of a system. This can lead to threats to users' information security and losses of the system owners. There are methods to detect attacks in recommendation systems, but they require permanent repetitive checks of all users' profiles, which is a rather resource-intensive operation. At the same time, these methods do not contain any proposals as for determining the optimal frequency of attack checks. However, a properly chosen frequency of such checks will not overload a system too much and, at the same time, will provide an adequate level of its operational security.

A mathematical model of the dynamics of states of a recommendation system under conditions of an information attack with the use of the mathematical apparatus of Markovian and semi-Markovian processes was developed. The developed model makes it possible to study the influence of profile injection attacks on recommendation systems, in particular, on their operation efficiency and amount of costs to ensure their information security. The practical application of the developed model enables calculating for recommendation systems the optimum frequency of information attack check, taking into consideration the damage from such attacks and costs of permanent inspections.

Based on the developed mathematical model, the method for determining total costs of a recommendation system as a result of monitoring its own information security, neutralization of bot-networks activity and as a result of information attacks was proposed.

A method for determining the optimal frequency of checking a recommendation system for information attacks to optimize the overall costs of a system was developed. The application of this method will enable the owners of websites with recommendation systems to minimize their financial costs to provide their information security

Keywords: recommendation system, information security, bot-network, Markovian processes, semi-Markovian processes

UDC 004.492.3: 519.711
DOI: 10.15587/1729-4061.2020.209047

DEVELOPING A MODEL OF THE DYNAMICS OF STATES OF A RECOMMENDATION SYSTEM UNDER CONDITIONS OF PROFILE INJECTION ATTACKS

Y. Meleshko
PhD, Associate Professor*
E-mail: elismeleshko@gmail.com
O. Drieiev
PhD, Associate Professor*
E-mail: drey.sanya@gmail.com
M. Yakymenko
PhD, Associate Professor*
E-mail: m.yakymenko@gmail.com
D. Lysytsia
PhD
Department of Computer Engineering and Programming
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
E-mail: lysytsia-mail@ukr.net
*Department of Cybersecurity and Software
Central Ukrainian National Technical University
Universytetskyi ave., 8, Kropyvnytskyi, Ukraine, 25006

Received date 20.05.2020
Accepted date 17.07.2020
Published date 28.08.2020

1. Introduction

Recommendation systems are increasingly often used on various web-resources and are becoming their important part, as well as search sub-systems, sometimes complementing them, and sometimes creating an alternative to them [1, 2]. They are most often used to form a news feed in social networks [2, 3], and to create recommendation lists for users of content websites and online stores [1]. With the help of recommendation systems, a user finds more quickly the content he needs, and the owner increases visiting his web-resource, and consequently, his own profit [1, 4].

Various informational impacts are often implemented through social networks [5, 6], and recommendation systems as their component have become one of the goals for information attacks to perform such influences [7, 8]. By making a successful attack on the recommendation system of a social network, one can change the content and order of showing the objects in news feeds to the system's users. This can be used for marketing, political, or fraudulent purposes.

The main type of information attacks on recommendation systems is the profile injection attacks [7–9]. These attacks are aimed at changing ratings, and thus at changing the frequency of showing certain objects of a system

in recommendations. To implement the described actions, the bot-networks are used, because only a certain set of profiles in a system can affect the formation of recommendations by their cohesive actions [8, 9]. If an attacker manages to increase object getting to the recommendation list, a target object is highly likely to become more well-known, popular, and demanded with users. Thus, one can promote certain products, services, or information. The goal of an attacker can be the opposite – to decrease object getting to the recommendation list. This will enable it to fight competitors, reducing the popularity of their content. Therefore, attacks on recommendation systems can lead to threats to users' information security and damage to the owners of a system.

Of course, there are some methods to detect and neutralize attacks in recommendation systems [1, 10–13], but they require permanent repeated checks of all profiles of users, which is a rather resource-intensive operation. At the same time, these methods have no proposals for determining the optimal frequency of attack check. However, properly chosen frequency of such checks will not overload a system and, at the same time, will provide an adequate level of its operational security.

On the one hand, the state of information security of a recommendation system should be constantly monitored to detect timely new bot profiles, which can appear and be activated in a system at any time. On the other hand, periodic checks should not be too frequent so as not to overload a system and not to slow down its work. In addition, too frequent attack checks of a system can significantly increase the financial costs of website owners for using computing resources.

Therefore, to solve the problem of determining the optimal frequency of attack checks of a recommendation system is a relevant scientific and practical task. Its solution will minimize the costs of providing information security for recommendation systems while maintaining its sufficient level.

2. Literature review and problem statement

Papers [7–9] studied the causes and general principles of information attacks on recommendation systems. The research results show that the main type of information attacks on recommendation systems is the profile injection attacks.

Profile injection attacks are information attacks that involve creating bot-networks that change the frequency of target objects of a recommendation system getting to recommendation lists [1, 7–9]. At the stage of preparation for an attack, bots may collect statistics about system users, using a recommendation list provided by a system in response to their certain actions [1, 10]. Such a method of information reception was called the Probe Attack, according to papers [1, 7–9], it can be considered an optional initial stage for a profile injection attack.

Papers [1, 10–13] address the methods for detection and neutralization of profile injection attacks in recommendation systems. These methods are based on identifying and neutralizing bot profiles based on clustering and machine learning algorithms. We can conclude from these works that the methods for protecting recommendation systems from information attacks are developed based on the known models of such attacks. The very first models of attacks on recommendation systems were proposed in [8], these are Random Attack and Average Attack models. The following papers [1, 14–17] explore more complex and information-intensive attacks, such as the Popular Attack, Bandwagon Attack, Segment Attack, etc. Based on the known attack models, the methods for detection of bots are developed, as they are based on the features of their behavior, characteristic of a certain model of an attack on a recommendation system.

The studies focusing on the detection of bot profiles in recommendation systems do not raise and resolve the problem of how often a system should be checked for bots. The reason for this may be the lack of developed models of recommendation systems during information attacks. This makes it impossible to determine the impact of the frequency of checking attacks on a recommendation system and its operational efficiency.

However, as the research shows [1, 7–9], the recommendation systems applying the collaborative filtering methods [18–21] are often subjected to profile injection attacks and are very vulnerable to them. This is because such methods use feedback from users that can be forged by using a bot network. There are many methods for filtering data for recommendation systems, and they are all, to a different extent, vulnerable to information attacks [1, 7]. At the same time, almost all modern recommendation systems are complex hybrids of different data filtering methods, most of which are the most common methods of collaborative filtering [1, 22]. Thus, almost all modern recommendation systems are vulnerable to profile injection attacks and are often under their influence. Detection and neutralization of information attacks require the use of additional computing resources [1, 11], and therefore additional financial costs for website owners.

Search for and research into the existing models of operation of recommendation systems show that the available models can be classified into the following:

– models of the formation of recommendation lists in recommendation systems [1, 2, 4, 18–23];

– models of hybridization of recommendation systems [22];

– models of behavior of users of recommendation systems [1, 18–23];

– models of dynamics of preferences of recommendation systems users in time [1, 23].

Based on the conducted study of sources, we can conclude about the absence of mathematical models of recommendation systems during information attacks, which complicates the development of qualitative subsystems of information security of such systems. At the same time, the vast majority of existing recommendation systems require protection from information profile injection attacks.

The important data for the development of the information security subsystem of a recommendation system and optimization of costs of its owners are data on the dynamics of the system's states under conditions of an information attack. The model of dynamics of a recommendation system would make it possible to study better the impact of information attacks on its operation and the costs of the owners in various attack-caused states of a system. It would allow reasonable choosing the frequency of bot-checks of a recommendation system.

Thus, the development of a mathematical model of dynamics of states of a recommendation system in the context of information attacks will enable solving the issue of determining the optimal frequency of system checking for an information attack to optimize the costs of the system owners.

3. The aim and objectives of the study

The aim of this research is to develop a mathematical model of dynamics of states of a recommendation system under conditions of information profile injection attacks. The practical application of the developed mathematical model will make it possible to calculate the optimum frequency of checks for the existence of information attacks for recommendation systems, taking into consideration their individual parameters, for subsequent neutralization of existing bots.

To achieve the set goal, the following tasks should be solved:

– to conduct research into general principles of information profile injection attacks on recommendation systems and the methods for their detection and neutralization;

– to develop a set of possible states of a recommendation system in the context of information profile injection attacks and analytical ratios to calculate the probabilities of a system being in these states at a random time;

– to develop the method to determine the costs of the recommendation system owner in the face of profile injection attacks and the method for determining the optimal frequency of information attack check of a system to optimize these costs.

4. Studying the general principles of information profile injection attacks on recommendation systems and methods for their detection and neutralization

Profile injection attacks on recommendation systems aim to change the ratings of one or more objects in a system. The goal of an attack may be to increase the ratings of their goods (content), reduce the ratings of competitors' goods (competitors' content), or both.

To make this influence, an attacker should quite accurately simulate the actions of ordinary users so as not to be detected. An attack-robust recommendation system should work so that the result from attackers' actions should be so ineffective that they could have no stimuli to continue attacks, and authentic users continued to receive relevant undistorted recommendations.

An attack on a recommendation system will be considered the coordinated efforts of a large number of bot profiles to offset its operation results so that a group of users or all users could start receiving recommendations that promote attack objects.

The general principle of a profile injection attack on a recommendation system, which uses feedback from users in the form of estimates of recommendation objects, on the example of increasing the rating of one object, is shown in Fig. 1.

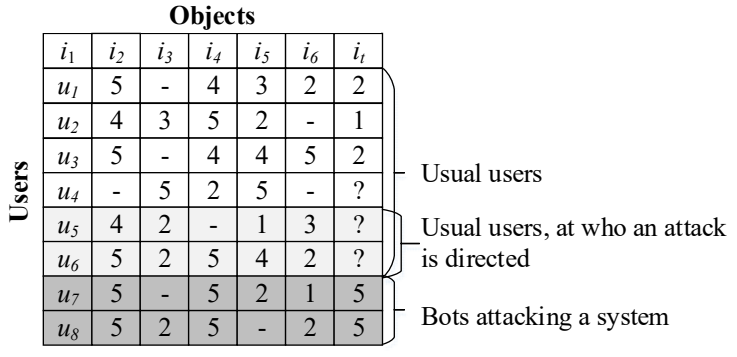

Fig. 1. General principle of profile injection attack on recommendation systems with collaborative filtration

Fig. 1 shows an example of a part of the rating database of an attacked recommendation system. A recommendation system is attacked by a bot network represented by users' profiles u_7 and u_8. The question mark marks the unknown values of estimates (users have not yet assessed the target object), which a system will try to predict during the generation of guidelines for users u_5 and u_6 and object i_t, which is the target of bot network attack. If a system predicts a positive estimate for an object i_t, it is highly likely to fall into recommendation lists for given users and they will pay attention to it. That is why bots give positive estimates to object i_t to increase its rating. And other objects of a system are given the estimates similar to those given by users u_5 and u_6. This is done to get a positive correlation with target users and a high coefficient of similarity to them, which a recommendation system will take into account when formulating recommendations to target users. Since ordinary users, similar to users u_5 and u_6, negatively assessed object i_t, then without bots attack, a recommendation system would predict a low estimate to this object. And, in this case, it would not get to the recommendations specified by users.

In order to neutralize this attack, it is necessary to determine which profiles are bots without taking into consideration their estimates when forming the recommendation list.

The overall model of the profile of a bot that attacks a recommendation system can be represented as follows (Fig. 2).

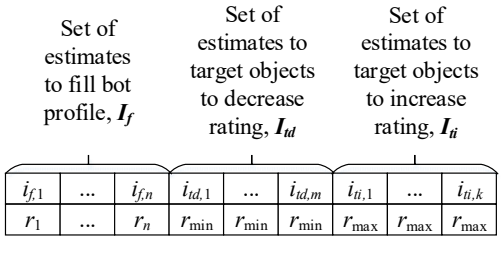

Fig. 2. Model of bot profile attacking a recommendation system

As Fig. 2 shows, the bot profile contains the following types of estimates:

– estimates to objects from set I_f. These estimates are given to simulate the actions of actual users. An attacker does not wish to change the ratings from this set. On the contrary, he tries to choose for them the values that are most

similar to the actual ones for a target group of users, who he is eager to influence;

– estimates to objects from set I_{ti}. These are the maximum (or close to them) estimates in the system for target objects, the rating of which an attacker seeks to increase;

– estimates of objects from set I_{td}. These are the minimum (or close to them) estimates in the system for target objects, the rating of which an attacker seeks to decrease.

The number of target objects in a bot can vary from 1 to K, and the number of objects to fill the profile – from 0 to N.

Bot actions can produce results only when the vast majority of bots give estimates on all target objects, and in this case, bots will not be detected and neutralized. The minimum required number of bots in a network, which will allow reaching the set goal depends on the algorithms of a recommendation system and can be determined by an attacker only experimentally.

There are several approaches to detecting bot profiles:

1. Profile clustering. Detection of bot profiles can be considered as a problem of binary classification of system profiles [1, 8, 10] with two possible results for each profile, specifically:

– authentic user profile;

– profile of a bot created to attack a system (Attack).

To create such a classifier, various methods of data clustering can be used, as well as various machine learning methods, which learn on a training sample of profiles, which contain both authentic profiles and bot profiles.

2. Analysis of individual profile statistics. The distribution of estimates in a bot profile is highly likely to be different from the distribution of estimates in authentic users' profiles. Although it is advantageous for an attacker to create bot profiles as similar to the profiles of regular system users as possible, he can never have enough information and resources to eliminate completely the differences between bots and normal users.

The features of a bot profile can be the following statistical characteristics [1, 8]: for example, the deviation from the mean value of estimates is greater than usual, some group of profiles has higher similarity to the checked profile than usual.

To protect a recommendation system from information attacks, the data of the profiles defined as Attack must be removed from the computations of rating prediction and recommendations creation so that they do not influence these processes in a system.

The efficiency of attack neutralizing can be assessed by a shift in the forecast of target object ratings before and after detecting an attack and bot profiles removal from the process of recommendation system computation [1, 8, 10, 12].

Predominantly in existing studies, it is proposed to consider the detection of an attack on a recommendation system identical to the detection of bot profiles [1, 8, 10–13].

Since detection of bot profiles, based on the conducted study, is quite a resource-intensive task, it is proposed in this research to divide the problem of protecting a recommendation system from information profile injection attack into two parts:

– attack detection;

– detection and neutralization of bot profiles.

Attack detection may be a less resource-intensive task and involve monitoring the dynamics of ratings of system objects, all of them or only those crucial in terms of information security. If the ratings of objects begin to change rapidly and new estimates leading to a change in ratings do not correspond to the previous average estimates of objects, it is necessary to check for bots among users who started to give such estimates to objects. This approach will reduce the number of users' profile checks. Firstly, because it will be necessary to check them only when the suspicion of an attack is detected. Secondly, because it will be necessary to check the profiles of not all users, but only of those engaged in suspicious activity.

After the detection of bot profiles, it is necessary to neutralize these profiles by removing their information from the database used for the formation of recommendation lists. Thus, the estimates they gave and the actions they performed (views, comments, etc.) will not affect the ratings of the objects of a system and forecasting recommendations.

5. Development of a mathematical model of the dynamics of a recommendation system states under conditions of information profile injection attack

A set of possible states of a recommendation system in the context of information profile injection attacks and analytical ratios to calculate the probability of a system being in these states at the random time were developed. Taking into account the conducted study of the threats to information security of recommendation systems and the ways to detect and neutralize the threats, we propose the following set of states of a recommendation system in terms of information security:

1) Normal operation. In this mode, there are additional costs for the organization of information attack detection, costs are proportional to the time of the system operation in the current state, and intensity of control measures: vtL_1.

2) A system was attacked. There are active bot-networks in a system. Bots in a system were not detected, recommendations are distorted under their influence. In this operation mode, the losses from the activity of tL_2 bots are accumulated in the time proportion. At the same time, checks for an information attack with losses tL_1 are conducted.

3) The system fights back an attack. The existence of an information attack was detected. Losses from incorrect recommendations continue tL_2. Resources are spent on the search and elimination of bots. In this mode, resources tL_3 to organize the return of the system operation to the normal state (1) are additionally consumed in proportion to operation time.

The graph of the system is shown in Fig. 3.

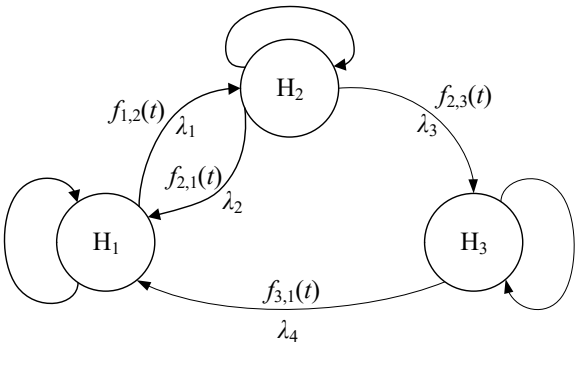

Fig. 3. Graph of the dynamics of states of a recommendation system under conditions of an information attack

The methodology of probabilistic analysis of the dynamics of states of multidimensional Markovian and semi-Markovian dynamical systems, developed in paper [24], was used to develop a mathematical model of dynamics of states of a recommendation system.

Consider the possible scenarios that may occur with a recommendation system that is vulnerable to information attacks.

A system is in working condition (1). A system can transfer to state (2), the probability of this transition is a random process with flow intensity λ_1. Then the distribution of density of system being in state (1) before the transition to state (2) will have the form: $f_{1,2}(t)=\lambda_1 e^{-\lambda_1 t}$. Transition from state (1) to state (3) is hardly probable, given that the time of the beginning of an attack on a system cannot coincide the time of detection of the fact of system damage. That is why there is no flow from state (1) to state (3): $f_{1,3}(t)=0$. But state (2) can change in two ways:

1) an attack was unnoticed and in some time a system got stabilized by itself into state (1) $f_{2,1}(t)=p_{2,1}\cdot\lambda_2 e^{-\lambda_2 t}$, probability $p_{2,1}$, which determines that the process will develop in this way exactly, was added to the distribution;

2) an attack was noticed, active counteractions are conducted as for the fact of attack existence – a system transferred to state (3) $f_{2,3}(t)=p_{2,3}\cdot\lambda_3 e^{-\lambda_3 t}$; this sequence of events is the supplement to scenario 1, which is determined by a multiplier-probability of event continuation with the specified probability. Due to the use of the sub-system of detection of an information attack, this probability is higher than 80 %, that is why we will accept the lower boundary as $p_{2,3}$=0.8, and probability $p_{2,1}$=1–$p_{2,3}$=1–0.8=0.2.

If a system is in state (3), after a while, it returns to the normal operation mode to state (1). Even in the case of an attack on a recommendation system in state (3), it can be ignored, because an attack is quite a long process, and a system is sure to return to state (1) before the transition to state (2). That is why the densities of probability to find a recommendation system in another state over time t are $f_{3,1}(t)=\lambda_4 e^{-\lambda_4 t}$, $f_{3,2}(t)=0$.

We designate the probability of a system to be in state (j) over time t as $G_{i,j}(t)$, i,j=1, 2, 3, if a system was in state (i) at the initial moment of time. Then one can write down the system of integral equations as:

$$\begin{cases}
G_{1,1}(t)=\left(1-\int f_{1,2}(\tau)d\tau-\int f_{1,3}(\tau)d\tau\right)+\int f_{1,2}(\tau)\cdot G_{2,1}(t-\tau)d\tau+\int f_{1,3}(\tau)\cdot G_{3,1}(t-\tau)d\tau,\\
G_{2,1}(t)=\int f_{2,1}(\tau)\cdot G_{1,1}(t-\tau)d\tau+\int f_{2,3}(\tau)\cdot G_{3,1}(t-\tau)d\tau,\\
G_{3,1}(t)=\int f_{3,1}(\tau)\cdot G_{1,1}(t-\tau)d\tau+\int f_{3,2}(\tau)\cdot G_{2,1}(t-\tau)d\tau,\\
G_{1,2}(t)=\int f_{1,2}(\tau)\cdot G_{2,2}(t-\tau)d\tau+\int f_{1,3}(\tau)\cdot G_{3,2}(t-\tau)d\tau,\\
G_{2,2}(t)=\left(1-\int f_{2,1}(\tau)d\tau-\int f_{2,3}(\tau)d\tau\right)+\int f_{2,1}(\tau)\cdot G_{1,2}(t-\tau)d\tau+\int f_{2,3}(\tau)\cdot G_{3,2}(t-\tau)d\tau,\\
G_{3,2}(t)=\int f_{3,1}(\tau)\cdot G_{1,2}(t-\tau)d\tau+\int f_{3,2}(\tau)\cdot G_{2,2}(t-\tau)d\tau,\\
G_{1,3}(t)=\int f_{1,2}(\tau)\cdot G_{2,3}(t-\tau)d\tau+\int f_{1,3}(\tau)\cdot G_{3,3}(t-\tau)d\tau,\\
G_{2,3}(t)=\int f_{2,1}(\tau)\cdot G_{1,3}(t-\tau)d\tau+\int f_{2,3}(\tau)\cdot G_{3,3}(t-\tau)d\tau,\\
G_{3,3}(t)=\left(1-\int f_{3,1}(\tau)d\tau-\int f_{3,2}(\tau)d\tau\right)+\int f_{3,1}(\tau)\cdot G_{1,3}(t-\tau)d\tau+\int f_{3,2}(\tau)\cdot G_{2,3}(t-\tau)d\tau.
\end{cases} \quad (1)$$

Here, a probability of the $\left(1-\int f_{1,2}(\tau)d\tau-\int f_{1,3}(\tau)d\tau\right)$ form means that an event of transition to another state over time t has not taken place. Due to this, the system is independent and allows for non-trivial solutions.

To solve this system of equations, one can use the Laplace transform, where the transformation result will be denoted with suffix ^. Considering the transformation properties makes it possible to get the equation system in the following form:

$$\begin{cases}
\hat{G}_{1,1}(s)=\dfrac{\left(1-\hat{f}_{1,2}(s)-\hat{f}_{1,3}(s)\right)}{s}+\\
+\hat{f}_{1,2}(s)\cdot\hat{G}_{2,1}(s)+\hat{f}_{1,3}(s)\cdot\hat{G}_{3,1}(s),\\
\hat{G}_{2,1}(s)=\hat{f}_{2,1}(s)\cdot\hat{G}_{1,1}(s)+\hat{f}_{2,3}(s)\cdot\hat{G}_{3,1}(s),\\
\hat{G}_{3,1}(s)=\hat{f}_{3,1}(s)\cdot\hat{G}_{1,1}(s)+\hat{f}_{3,2}(s)\cdot\hat{G}_{2,1}(s),\\
\hat{G}_{1,2}(s)=\hat{f}_{1,2}(s)\cdot\hat{G}_{2,2}(s)+\hat{f}_{1,3}(s)\cdot\hat{G}_{3,2}(s),\\
\hat{G}_{2,2}(s)=\dfrac{\left(1-\hat{f}_{2,1}(s)-\hat{f}_{2,3}(s)\right)}{s}+\\
+\hat{f}_{2,1}(s)\cdot\hat{G}_{1,2}(s)+\hat{f}_{2,3}(s)\cdot\hat{G}_{3,2}(s),\\
\hat{G}_{3,2}(s)=\hat{f}_{3,1}(s)\cdot\hat{G}_{1,2}(s)+\hat{f}_{3,2}(s)\cdot\hat{G}_{2,2}(s),\\
\hat{G}_{1,3}(s)=\hat{f}_{1,2}(s)\cdot\hat{G}_{2,3}(s)+\hat{f}_{1,3}(s)\cdot\hat{G}_{3,3}(s),\\
\hat{G}_{2,3}(s)=\hat{f}_{2,1}(s)\cdot\hat{G}_{1,3}(s)+\hat{f}_{2,3}(s)\cdot\hat{G}_{3,3}(s),\\
\hat{G}_{3,3}(s)=\dfrac{\left(1-\hat{f}_{3,1}(s)-\hat{f}_{3,2}(s)\right)}{s}+\\
+\hat{f}_{3,1}(s)\cdot\hat{G}_{1,3}(s)+\hat{f}_{3,2}(s)\cdot\hat{G}_{2,3}(s).
\end{cases} \quad (2)$$

Since the initial state of a system is known and it is state (1), it is enough to determine the following functions: $G_{1,1}(t)$, $G_{1,2}(t)$, $G_{1,3}(t)$.

The solution of the system of equations is:

$$\hat{G}_{1,1}(s)=\frac{\left(\hat{f}_{1,3}(s)+\hat{f}_{1,2}(s)-1\right)\left(\hat{f}_{2,3}(s)\hat{f}_{3,2}(s)-1\right)}{\left(\left(\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\hat{f}_{2,1}(s)\right)\hat{f}_{3,2}(s)+\left(\hat{f}_{1,2}(s)\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\right)\hat{f}_{3,1}(s)+\hat{f}_{1,2}(s)\hat{f}_{2,1}(s)-1\right)\cdot s},$$

$$\hat{G}_{1,2}(s)=\frac{\left(\hat{f}_{1,3}(s)\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\hat{f}_{2,1}(s)-\hat{f}_{1,3}(s)\right)\hat{f}_{3,2}(s)+\hat{f}_{1,2}(s)\hat{f}_{2,3}(s)+\hat{f}_{1,2}(s)\hat{f}_{2,1}(s)-\hat{f}_{1,2}(s)}{\left(\left(\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\hat{f}_{2,1}(s)\right)\hat{f}_{3,2}(s)+\left(\hat{f}_{1,2}(s)\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\right)\hat{f}_{3,1}(s)+\hat{f}_{1,2}(s)\hat{f}_{2,1}(s)-1\right)\cdot s}, \quad (3)$$

$$\hat{G}_{1,3}(s)=\frac{\left(\hat{f}_{1,2}(s)\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\right)\hat{f}_{3,2}(s)+\left(\hat{f}_{1,2}(s)\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\right)\hat{f}_{3,1}(s)-\hat{f}_{1,2}(s)\hat{f}_{2,3}(s)-\hat{f}_{1,3}(s)}{\left(\left(\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\hat{f}_{2,1}(s)\right)\hat{f}_{3,2}(s)+\left(\hat{f}_{1,2}(s)\hat{f}_{2,3}(s)+\hat{f}_{1,3}(s)\right)\hat{f}_{3,1}(s)+\hat{f}_{1,2}(s)\hat{f}_{2,1}(s)-1\right)\cdot s}.$$

Subsequently, it is possible to use

$$f_{1,2}(t)=\lambda_1 e^{-\lambda_1 t},$$

$$f_{1,3}(t)=0,$$

$$f_{2,1}(t)=p_{2,1}\cdot\lambda_2 e^{-\lambda_2 t},$$

$$f_{2,3}(t)=p_{2,3}\cdot\lambda_3 e^{-\lambda_3 t},$$

$$f_{3,1}(t)=\lambda_4 e^{-\lambda_4 t},$$

$$f_{3,2}(t)=0,$$

for which the Laplace transform will have the form:

$$f^{\wedge}_{1,2}(s)=\lambda_1/(s+\lambda_1),\ f^{\wedge}_{1,3}(s)=0,\ f^{\wedge}_{2,1}(s)=p_{2,1}\cdot\lambda_2/(s+\lambda_2),$$

$$f^{\wedge}_{2,3}(s)=p_{2,3}\lambda_3/(s+\lambda_3),\ f^{\wedge}_{3,1}(s)=\lambda_4/(s+\lambda_4),$$

$$f^{\wedge}_{3,2}(s)=0.$$

Then the Laplace transform for sought-after functions is:

$$G^{\wedge}_{1,1}(s)=\frac{(\lambda_2+s)(\lambda_3+s)(\lambda_4+s)}{s\cdot\left(s^3+k_0+s^2k_2+s\cdot\left(k_1+\lambda_2k_4+\lambda_1\left(k_3-p_{2,1}\lambda_2\right)\right)+\lambda_1\left(p_{2,1}k_1+p_{2,3}\lambda_2k_4\right)\right)},$$

$$G^{\wedge}_{1,2}(s)=\frac{\lambda_1\left(s+\lambda_2-p_{2,1}\lambda_2+p_{2,1}\lambda_3\right)(\lambda_4+s)}{s\cdot\left(s^3+k_0+s^2k_2+s\cdot\left(k_1+\lambda_2k_4+\lambda_1\left(\lambda_2-p_{2,1}\lambda_2+k_4\right)\right)+\lambda_1\left(p_{2,1}k_1+p_{2,3}\lambda_2k_4\right)\right)}, \quad (4)$$

$$G^{\wedge}_{1,3}(s)=\frac{p_{2,3}\lambda_1\lambda_3(\lambda_2+s)}{s\cdot\left(s^3+k_0+s^2k_2+s\cdot\left(k_1+\lambda_2k_4+\lambda_1\left(\lambda_2-p_{2,1}\lambda_2+k_4\right)+\lambda_1\left(p_{2,1}k_1+p_{2,3}\lambda_2k_4\right)\right)\right)},$$

where

$$k_0=\lambda_2\lambda_3\lambda_4,\ k_1=\lambda_3\lambda_4,$$

$$k_2=\lambda_1+\lambda_2+\lambda_3+\lambda_4,\ k_3=\lambda_2+\lambda_3+\lambda_4,\ k_4=\lambda_3+\lambda_4.$$

Since the analytical solution to the equation is quite complicated and cumbersome, we propose to use numerical methods. Existing specific values make it possible to find the roots either accurately, or approximately, so, for example, the following parameters will be used: λ_1=0.01; λ_2=0.01; λ_3=0.1; λ_4=0.1; p_{21}=0.2; p_{23}=0.8, here λ is the event intensity and is responsible for the time of a system being in a certain state. For example, at λ=0.01, we will observe on average one event on 100 conditional time units. In actual recommendation systems, the value of these intensities and probabilities can be any, their values depend on the system parameters and the fact of the existence of bot-networks parameters. These values can be determined by the owners of a recommendation system based on the analysis of statistical data available to system administrators.

As a result of the substitution, we have the following Laplace images of sought-after functions:

$$G^{\wedge}_{1,1}(s)=\frac{25}{34\cdot s}+$$
$$+\frac{562{,}500\cdot s^2+102{,}500\cdot s+3{,}500}{17\cdot\left(125{,}000\cdot s^3+27{,}500\cdot s^2+1{,}760\cdot s+17\right)},$$

$$G^{\wedge}_{1,2}(s)=\frac{7}{34\cdot s}+$$
$$+\frac{437{,}500\cdot s^2+75{,}000\cdot s+3{,}440}{17\cdot\left(125{,}000\cdot s^3+27{,}500\cdot s^2+1{,}760\cdot s+17\right)},$$

$$G^{\wedge}_{1,3}(s)=\frac{1}{17\cdot s}+$$
$$+\frac{125{,}000\cdot s^2+27{,}500\cdot s+60}{17\cdot\left(125{,}000\cdot s^3+27{,}500\cdot s^2+1{,}760\cdot s+17\right)}.$$

As a result, each of the sought-after probabilities has the summand in the form of a number divided by s, which corresponds to the constant. That is, for a system that stabilized in time, probabilities of detecting a system in states (1) to (3), respectively, are equal to $G_{1,1}$=25/34, $G_{1,2}$=7/34, and $G_{1,3}$=1/17. These probabilities totally make up 1, which is one of the arguments for correctness of obtained dependences.

The next fraction, which was represented in the second summand of Laplace images of $G^{\wedge}_{1,1}(s)$, $G^{\wedge}_{1,2}(s)$, and $G^{\wedge}_{1,3}(s)$, can be decomposed into elementary. To do this, it is necessary to find the roots of the denominator:

$$125{,}000\cdot s^3+27{,}500\cdot s^2+$$
$$+1{,}760\cdot s+17=0,$$

hence:

$$s_1\approx-0.0117,\ s_2\approx0.02825\cdot i-$$
$$-0.1042,\ s_3\approx$$
$$\approx-0.02825\cdot i-0.1042.$$

All real parts of the roots have negative values that correspond to exponentially decreasing dependences. That is, the probabilities over time converge to the specified constants.

Therefore, the sought-after probabilities in the general case can be determined from the following formulas:

$$G_{1,1}=\frac{\lambda_2\lambda_3\lambda_4}{Z},$$

$$G_{1,2}=\frac{\lambda_1\left(p_{2,3}\left(\lambda_2-\lambda_3\right)+\lambda_3\right)\lambda_4}{Z},$$

$$G_{1,3}=\frac{p_{2,3}\lambda_1\lambda_2\lambda_3}{Z}, \quad (5)$$

where

$$Z=\left(\lambda_1+\lambda_2\right)\lambda_3\lambda_4+p_{2,3}\lambda_1\left(\lambda_2\left(\lambda_3+\lambda_4\right)-\lambda_3\lambda_4\right).$$

The case when a recommendation system is modeled by semi-Markovian processes was considered as well. The Erlang distributions of second and higher-order are often used as an event flow model, which makes it possible to simulate semi-Markovian processes. Distribution is the product of the sum of two (for second-order distribution) of exponential distributions that in the Laplace arithmetic are represented as a product of images:

$$e(t)=\int_0^t f(\tau)f(t-\tau)\mathrm{d}\tau,$$

$$\hat{e}(s)=\hat{f}(s)\hat{f}(s),$$

$$\hat{e}(s)=\frac{\lambda^2}{(s+\lambda)^2}. \quad (6)$$

As a result of using the magnitudes of flows λ_1=0.01, λ_2=0.01, λ_3=0.1, λ_4=0.1, we will have the following expressions: where k=10^8.

$$G^{\wedge}_{1,1}(s)=\frac{25}{34\cdot s}+\frac{1}{17}\times\frac{2{,}812.5\cdot k\cdot s^6+1{,}237.5\cdot k\cdot s^5+214.375\cdot k\cdot s^4+18.24\cdot k\cdot s^3+76{,}468{,}750\cdot s^2+1{,}312{,}500\cdot s+8{,}125}{625\cdot k\cdot s^7+275\cdot k\cdot s^6+47.875\cdot k\cdot s^5+4.1525\cdot k\cdot s^4+1{,}860.05\cdot k\cdot s^3+415{,}200\cdot s^2+4{,}280\cdot s+17},$$

$$G_{1,2}^{\wedge}(s)=\frac{7}{34\cdot s}+\frac{1}{17}\times\frac{2{,}187.5k\cdot s^6+962.5k\cdot s^5+166.5k\cdot s^4+14.0875k\cdot s^3+58{,}718{,}250\cdot s^2+1{,}084{,}300\cdot s+7{,}330}{625k\cdot s^7+275k\cdot s^6+47.875k\cdot s^5+4.1525k\cdot s^4+18{,}600{,}500\cdot s^3+415{,}200\cdot s^2+4{,}280\cdot s+17},$$

$$G_{1,3}^{\wedge}(s)=\frac{1}{17\cdot s}+\frac{1}{17}\times\frac{625k\cdot s^6+275k\cdot s^5+47.875k\cdot s^4+4.1525k\cdot s^3+17{,}750{,}500\cdot s^2+228{,}200\cdot s+795}{625k\cdot s^7+275k\cdot s^6+47.875k\cdot s^5+4.1525k\cdot s^4+18{,}600{,}500\cdot s^3+415{,}200\cdot s^2+4{,}280\cdot s+17}.$$

It is important to note that the values of probabilities for a stabilized system are constant: 25/34, 7/34, 2/34. This is logical, because the probability of getting a system in this or that state over time that exceeds the system stabilization time does not depend on distribution, but only on the event flow. However, there are significant changes in transitional processes, the dynamics of which are determined by power fractions. Denominator's zeros are:

s_1=0.0034i–0.0104,

s_2=–0.0034i–0.0104,

s_3=0.0140i–0.0261,

s_4=–0.0140i–0.0261,

s_5=0.0059i–0.0796,

s_6=–0.0059i–0.0796,

s_7=–0.1079,

where all real parts are negative and guarantee convergence of changes in probabilities to constant values. By module, real parts of the roots are commensurate with the values of event flows, which means the stabilization of probabilities of a system of all at the occurrence of several most unlikely events.

As a result, when solving the problems of determining the dynamics of processes of a change in probability, it is advisable to significantly complicate the computation, however, in order to study the patterns in the operation of a stationary system, it is enough to check the stability of resulting solutions.

Thus, the model of dynamics of states of a recommendation system in the context of information attacks with the use of the mathematical apparatus of Markovian and semi-Markovian processes was developed.

6. Development of the method for determining the costs of a recommendation system in the context of profile injection attacks and the method for determining the optimal frequency of information attack check

The method to determine the costs that a recommendation system has as a result of monitoring its own information security and due to information attacks was developed.

Let us assume that in a situation when a recommendation system is in state (2), owing to the incorrectly created recommendations, the gains are lost in proportion to the time of its being in this state $C_1=tK_1$. Here, K_1 is the number of conditional monetary units (mon. units) per unit of time, lost by the system owner as a result of a successful attack of a bot- network. If an information attack check is performed, it is necessary to use additional computing resources, which can be expressed by costs $C_2=tK_2\lambda_3$. Here K_2 is the number of conditional monetary units per unit time, which the system owner loses as a result of using additional computing resources to make an information attack check of a system. Costs C_2 are proportional not only to the time of a system being in state (1) and (2), but also to the intensity of bots testing. The testing frequency corresponds to the frequency of bots' detection if a system was attacked (transition from state (2) to (3)). State (3) corresponds to the continuation of getting losses L_1.

Designate time t_1 as the share of time when we have losses L_1 due to active intervention of bots. Time t_2 will be designated as a share of time for bots intervention checks (existence of an information attack) with consuming resources L_2. Time t_3 is a share of time for identification of particular bot profiles and elimination of consequences of their activities with the consumption of computing resources tK_3. Here, K_1 is the number of conditional monetary units per unit of time, lost by the system owner as a result of using additional computing resources to identify particular bot profiles and neutralize their activities. Then the shares of time can be determined as the sum of probabilities:

– $t_1=G_{1,2}+G_{1,3}$ because in states (2) and (3) we have losses from the activity of bots;

– $t_2=G_{1,1}+G_{1,2}$ because in states (1) and (2) we have losses from bots activity testing;

– $t_3=G_{1,3}$ because only in state (3), there is an active search for bots and neutralization of their activity.

Probabilities $G_{1,1}$, $G_{1,2,}$ and $G_{1,3}$ are determined from formula (5).

Accordingly, full costs in a recommendation system will be:

$$L=\left(G_{1,2}+G_{1,3}\right)\cdot K_1+\left(G_{1,1}+G_{1,2}\right)\cdot K_2\lambda_3+G_{1,3}K_3. \qquad (7)$$

Coefficients K_1, K_2, K_3 are the parameters of the model, which depend on the structure and algorithms of a recommendation system, the volume of its database, computing capacities of computer systems, on which a system is deployed. These coefficients for each particular system will be different and can be determined and known only by the owners of a specific web-resource. K_2 and K_3 owners of a web- resource determine their hosting providers based on their tariff plans. K_1 is determined based on average statistical losses from the previous attacks of bot-networks, the consequences of which could be a loss of customers, a loss of advertising revenues, and losses to overcome the results of an attack, etc.

Thus, using formula (7), it is possible to determine complete losses of a recommendation system from information security "monitoring", neutralization of bots, and the activity of bot-networks.

The method for determining the optimal frequency of an information attack check of a recommendation system was developed in this research.

In the subsystem of the recommendation system security, it is possible to control the frequency of checking an information attack and bots' activities, which is responsible for the value of parameter λ_3.

In order to determine the optimal frequency of information attack check of a system v_{opt}, it is necessary to find such value λ_3, at which total losses of the L system will be minimal:

$$v_{opt} = \arg\min_{\lambda_3} L(\lambda_3) = \\ = \arg\min_{\lambda_3} \begin{bmatrix} (G_{1,2} + G_{1,3}) \cdot K_1 + \\ + (G_{1,1} + G_{1,2}) \cdot K_2 \lambda_3 + G_{1,3} K_3 \end{bmatrix}. \quad (8)$$

This equation is nonlinear, because of the impact of value λ_3 on coefficients G. That is why its solution in the general case is possible only by means of numerical methods or optimization methods.

Consider an example of determining the optimal frequency of information attack check of a system, using numerical methods.

For example, let us take the following values of all the types of costs of a recommendation system:

– K_1=5 mon. units/min;

– K_2=1 mon. units/min;

– K_3=2 mon. units/min.

Such values of costs are taken from the following consideration: the losses due to activity of bots K_1 are, as a rule, higher than costs of monitoring the state of system K_2 and for identification and neutralization of profiles of bots K_3. In addition, costs of monitoring a system with a view to detecting the existence of attacks K_2 are lower than the costs to identify and neutralize particular profiles of bots K_3.

The values of the rest of the constants remain the same as previously: λ_1=0.01; λ_2=0.01; λ_4=0.1; p_{21}=0.2; p_{23}=0.8.

Determine v_{opt} with the help of tabulation of the costs function (7) for λ_3=0; 0.05; 0.1; 0.15; 0.2; 0.25; 0.3, where the values of probabilities $G_{1,1}$, $G_{1,2}$ and $G_{1,3}$ are obtained from (5), the results are shown in Table 1.

The expression for the cost function at the specified values of parameters has the form of:

$$L(\lambda_3) = \\ = \frac{0.000195 + 0.0389\lambda_3 + 1.231\lambda_3^2 + 0.9375\lambda_3^3}{0.0000391 + 0.0125\lambda_3 + \lambda_3^2}.$$

Table 1

Example of computations to determine the optimal frequency of checking a recommendation system for information bots' attacks v_{opt}

$v=\lambda_3$	0.00	0.05	0.10	0.15	0.20	0.25	0.3
$G_{1,1}$	1/2	25/36	25/34	75/100	25/33	125/164	75/98
$G_{1,2}$	1/2	9/36	7/34	19/100	6/33	29/164	17/98
$G_{1,3}$	0	2/36	2/34	6/100	2/33	10/164	6/98
L	2.5	1.67	1.54	1.51	1.52	1.55	1.58

Graphic representation of the constructed points for the values of total losses of a recommendation system L at different values of frequency of information attack checks v, which are joined by a smooth curve, is shown in Fig. 4.

From Fig. 4 and Table 1, it can be concluded that the minimal total costs of a system will make up $L_{\min}$=1.51 mon. unit/min at the frequency of information attack check v_{opt}=0.16 1/min, which corresponds to periodicity of bots check T=$=1/\lambda_3$=6.25 min. If a search for an existing intervention into a recommendation system is conducted with higher intensity, the costs will increase due to additional computations, if the bots with less intensity are identified, there will be a situation with an increase in costs due to the incorrect operation of a system.

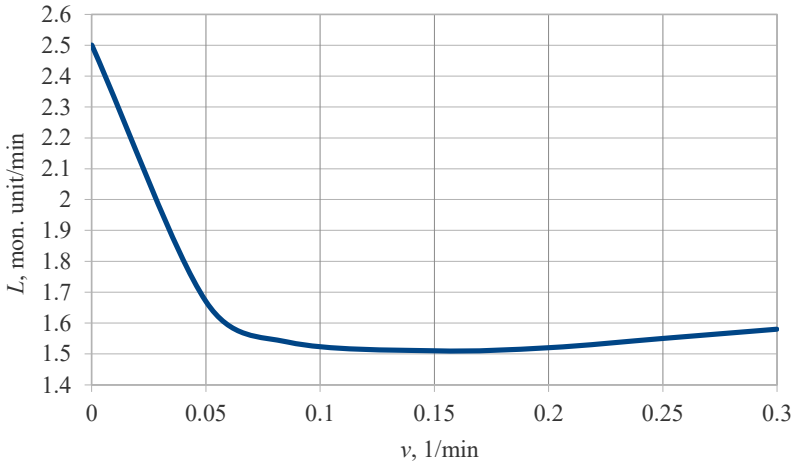

Fig. 4. Dependence of the amount of total costs of a recommendation system L on frequency of its information attack check v

If checking intensity for the explored example was maximum $v=\lambda_3$=1, i. e. checking continued constantly, the total losses of a system would reach L=2.18 mon. unit/min. That is, at the application of the optimal frequency of attack checking of a recommendation system, the total losses of a system decrease by (2.18–1.51)/2.18=30.7 %.

Thus, the method for determining the optimal frequency of an information attack check of a recommendation system was proposed. Using a specific example, the method for using the developed mathematical model describing the probabilistic dynamics of states of a recommendation system under conditions of information attacks was explored.

7. Discussion of results of the development of a model of dynamics of states of a recommendation system under conditions of information attacks

Thus, the research into general principles of information profile injection attacks on recommendation systems (Fig. 1, 2) and the methods for their detection and neutralization was conducted. It was proposed, in contrast to the existing approaches [1, 10–13], to divide the problem of protection of a recommendation system from information profile injection attacks into two parts: detection of an attack and detection and neutralization of bot profiles. This approach will reduce the number of checks of users' profiles. An information attack check can involve tracking the dynamics of objects' ratings and the detection of abnormal trends in it. Thus, it is possible to track the dynamics of ratings of all objects of a system or only those crucial for the protection against information attacks. In this case, it is necessary to check users' profiles to search for bots only when some sus-

picious changes in object ratings were detected and only of those users who affected the detected changes.

Based on the conducted research, we developed the mathematical model of the dynamics of states of a recommendation system under conditions of information attacks (Fig. 3, formulas (1) to (5)), which is original in comparison with the well-known models of recommendation systems [1, 2, 4, 18–23]. The developed mathematical model proposes the following set of operation states of a recommendation system: normal operation of system H_1, attacked system H_2, the system fights back an attack H_3. The graph of the dynamics of states of a recommendation system states in terms of information security was developed (Fig. 3). Transitions between system states, caused by the following processes, are possible:

1) implementation of attacks (transition $H_1 \rightarrow H_2$, flow intensity λ_1);

2) loss of relevance of bots' activity ($H_2 \rightarrow H_1$, λ_2);

3) attack detection ($H_2 \rightarrow H_3$, λ_3);

4) detection and neutralization of bots ($H_3 \rightarrow H_1$, λ_4). λ_3 is the parameter, the value of which is chosen by the system's administrator, it is directly the frequency of checking a system for the existence of attacks.

The intensity of flows λ_1, λ_2, λ_4 is determined by measurements and depends on the parameters of a system. For flows λ_2 and λ_4, it is possible to carry out direct measurements. λ_2 is determined as the inverse magnitude of the average period of the relevance of the attacked object of a system. λ_4 can be determined experimentally during test runs of the software for bots' detection and removal of the results of their activity. Event flow λ_1 corresponds to the frequency of attack implementation. Because some attacks can be undetected, this flow is difficult to estimate and it is clarified during the system operation.

The developed model contains a set of integral equations with respect to unknown functions that describe the probable dynamics of a system (1). The development of this mathematical model was based on the method for probabilistic analysis of dynamics of the states of multidimensional semi-Markovian dynamic systems, proposed in [24]. The equations (1) were solved with the help of Laplace transform, with the use of which the integral equations were replaced with the system of linear algebraic equations (2) that has the solution (3). With the use of representations for densities of transition distributions, the expressions for the Laplace transformants of conditional probabilities of transitions from state H_1 (4) were obtained. Unlike the example for two possible states [24], in this case, the reverse transition is quite cumbersome (since it is necessary to use formulas for the roots of algebraic equations of third and fourth powers). That is why the transition to the originals for conditional probabilities is performed for specific numerical values of parameters. The emphasis is placed on the ratio for stabilized values of probabilities (5) that are represented by first summands in the expressions for probability images. This is explained by the fact that the roots of denominators in decomposition into elementary fractions in the Laplace transform have negative values, which is why the summands, besides the first ones, will tend to zero during the transition to the originals of the Laplace transform. For semi-Markovian processes (6), which are modeled by Erlang distribution of the second and higher order, the values for stabilized probabilities have the same form (5). As a result of the numerical solution of integral equations, the obtained ratios for the calculation of the conditional probabilities $G_{1,1}$, $G_{1,2}$ and $G_{1,3}$ of finding a recommendation system in states H_1, H_2, and H_3 at an arbitrary moment of time t, if at the initial moment of time a system is in state H_1. The developed mathematical model contains the proposed principle of dividing the problem of protection of a recommendation system from profile injection attacks into two sub-problems:

1) attack detection;

2) detection and neutralization of bots' profiles.

The first sub-problem is represented by the transition from state H_2 to state H_3 and is characterized by flow intensity λ_3. The second one is represented by the transition from state H_3 to state H_1 and is characterized by flow intensity λ_4. If a system used the standard approach, when detection of an information attack and identification of bots' profiles is the same process, it is necessary to establish $\lambda_4=1$ for further use of the developed model. In this case, the transition from state H_2 to state H_3 will take place during finding bots' profiles. The transition from state H_3 to state H_1 will take place during bots' neutralization, which will always occur for all detected bots. Thus, both sub-problems are united into one sequential process. Ratios (1)–(5), obtained in the developed mathematical model enable solving the problems of assessing the efficiency of a recommendation system and cost-effectiveness of using computational resources under conditions of information attacks.

Based on the developed mathematical model, the method for determining the total costs of a recommendation system in the process of its operation was proposed (formula (7)). It was possible to calculate the complete costs of a system under conditions of an information attack due to the detection of a set of possible states, in which it can be, and to find the expressions to identify the probability of its being in these states. After all, in its each state a system suffers from various losses. Thus, a system suffers from losses from the bots' activities in states H_2 and H_3. It suffers from losses from monitoring for an information attack in states H_1 and H_2. In state H_3, there are losses from identification and neutralization of particular bots' profiles. The segments of time, on which certain costs appear, can be determined as the sums of corresponding probabilities. Determining total costs for providing information security of a recommendation system at its different parameters is a necessary step for the selection of optimal parameters of a system in terms of minimization of costs of its owners.

The method for determining the optimal frequency of information attack check of a recommendation system (formula (8), Table 1, Fig. 4), taking into consideration the limitation of computing resources for this check, was developed. This method makes it possible to determine the optimal frequency of attack check of a system at the known parameters of a recommendation system using numerical methods. To use it, it is necessary to know the cost of computational resources for the website owner, the amount of the required computing resources by the algorithms for information security monitoring and searching for bots, as well as the average losses from previous attacks of bots. The application of the developed method will make it possible to reduce the costs of the owner of a recommendation system for providing its information security.

8. Conclusions

1. It was proposed to divide the problem of protection of a recommendation system from information profile injection attacks into two parts: attack detection and detection and neutralization of bots' profiles. This division is advisable because detection of bots' profiles is quite a resource-intensive problem. This approach will reduce the number of checks of users' profiles. Firstly, this is because it will be necessary to check them only when the attack suspicions are detected. Secondly, it will be necessary to check the profiles of not all users, but only of those engaged in suspicious activity. An information attack check may be a less resource-intensive problem, which does not require the search for bots and involves tracking the dynamics of the ratings of objects and detection of abnormal trends in it. After revealing abnormal changes in objects' ratings, it is possible to check the profiles of the users who influenced the corresponding changes with a view to searching for bots among them.

2. The mathematical model of the dynamics of states of a recommendation system under conditions of information attacks was developed. The models of Markovian and semi-Markovian processes were chosen as the main tool of mathematical formalization. Within the mathematical model, a set of possible states, in which a recommendation system may be under conditions of information profile injection attack was developed. Three states of the recommendation system operation under conditions of an information attack were proposed, specifically, "normal state", "attacked system" and "a system fights back an attack". Possible transitions between these states were identified. Analytical ratios for calculation of probabilities of the recommendation system staying in its possible states at an arbitrary moment of time were developed. The developed mathematical model makes it possible to study the influence of information profile injection attacks on recommendation systems, on the accuracy and efficiency of their operation and the volume of costs of providing their information security.

3. Based on the developed mathematical model, we designed the method for determining total costs that a recommendation system has as a result of monitoring of its own information security, neutralization of the activity of bot-networks and as a result of information profile injection attacks. The formula for determining the total costs of a recommendation system under conditions of information profile injection attacks was offered. The developed method makes it possible at the known costs of computing resources and the known losses in attacks of bot-networks to determine the overall costs of servicing a security subsystem of a recommendation system. The method for determining the optimal frequency of checking a recommendation system for an information attack and bots' profiles to optimize the total costs of a system was developed. The proposed method is based on the use of numerical methods. The solution to a problem of determining the optimal frequency of checking a recommendation system for an information profile injection attack was considered using a specific example. If we know the average intensity of the flow of active bot-networks appearing in a recommendation system and the rate of operation of their detection algorithms, it is possible to reduce the total costs of a system by optimizing the attack search frequency. In this specific example, using the optimum frequency of attack check of a system lowers the total costs of system owners by 30.7 % compared to the constant check of a system. As the frequency of the appearance of active bot-networks in actual recommendation systems will not be continuous in time, the maximum frequency of attack checks will never be optimal. Thus, the application of the method for determining the optimal frequency of checking a recommendation system for an information attack will enable the owners of web-resources to minimize their financial costs of ensuring the information security of recommendation systems.

References

1. Ricci, F., Rokach, L., Shapira, B., Kantor, P. B. (Eds.) (2011). Recommender Systems Handbook. Springer, 842. doi: https://doi.org/10.1007/978-0-387-85820-3
2. Valois, C., Armada, M. (2011). Recommender Systems In Social Networks. JISTEM Journal of Information Systems and Technology Management, 8 (3), 681–716. doi: https://doi.org/10.4301/s1807-17752011000300009
3. Social networking and recommendation systems. Available at: https://courses.cs.washington.edu/courses/cse140/13wi/homework/hw4/homework4.html
4. He, J., Chu, W. W. (2010). A Social Network-Based Recommender System (SNRS). Annals of Information Systems, 47–74. doi: https://doi.org/10.1007/978-1-4419-6287-4_4
5. Kurban, A. (2016). Researches of modern information wars in online social networks. Informatsiyne suspilstvo, 23, 85–90. Available at: http://nbuv.gov.ua/UJRN/is_2016_23_15
6. Ulichev, O. S., Meleshko, Y. V., Sawicki, D., Smailova, S. (2019). Computer modeling of dissemination of informational influences in social networks with different strategies of information distributors. Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2019. doi: https://doi.org/10.1117/12.2536480
7. Lam, S. K., Riedl, J. (2004). Shilling recommender systems for fun and profit. Proceedings of the 13th Conference on World Wide Web - WWW '04. doi: https://doi.org/10.1145/988672.988726
8. O'Mahony, M. P., Hurley, N. J., Silvestre, G. C. M. (2002). Promoting Recommendations: An Attack on Collaborative Filtering. Database and Expert Systems Applications, 494–503. doi: https://doi.org/10.1007/3-540-46146-9_49
9. Kumari, T., Bedi, P. (2017). A Comprehensive Study of Shilling Attacks in Recommender Systems. International Journal of Computer Science Issues, 14 (4), 44–50. doi: https://doi.org/10.20943/01201704.4450
10. 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, 13 (5), e0196533. doi: https://doi.org/10.1371/journal.pone.0196533
11. Chirita, P.-A., Nejdl, W., Zamfir, C. (2005). Preventing shilling attacks in online recommender systems. Proceedings of the Seventh ACM International Workshop on Web Information and Data Management - WIDM '05. doi: https://doi.org/10.1145/1097047.1097061

12. 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). doi: https://doi.org/10.1109/ijcnn.2014.6889419
13. Williams, C. A., Mobasher, B., Burke, R. (2007). Defending recommender systems: detection of profile injection attacks. Service Oriented Computing and Applications, 1 (3), 157–170. doi: https://doi.org/10.1007/s11761-007-0013-0
14. Mobasher, B., Burke, R., Bhaumik, R., Williams, C. (2007). Toward trustworthy recommender systems. ACM Transactions on Internet Technology, 7 (4), 23. doi: https://doi.org/10.1145/1278366.1278372
15. Mobasher, B., Burke, R., Bhaumik, R., Williams, C. (2005). Effective attack models for shilling item-based collaborative filtering systems. In Proceedings of the WebKDD Workshop.
16. Kaur, P., Goel, S. (2016). Shilling attack models in recommender system. 2016 International Conference on Inventive Computation Technologies (ICICT). doi: https://doi.org/10.1109/inventive.2016.7824865
17. Gunes, I., Kaleli, C., Bilge, A., Polat, H. (2012). Shilling attacks against recommender systems: a comprehensive survey. Artificial Intelligence Review, 42 (4), 767–799. doi: https://doi.org/10.1007/s10462-012-9364-9
18. Mohammed, A. S., Meleshko, Y., Balaji B, S., Serhii, S. (2019). Collaborative Filtering Method with the use of Production Rules. 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). doi: https://doi.org/10.1109/iccike47802.2019.9004257
19. Su, X., Khoshgoftaar, T. M. (2009). A Survey of Collaborative Filtering Techniques. Advances in Artificial Intelligence, 2009, 1–19. doi: https://doi.org/10.1155/2009/421425
20. Jones, M. (2013). Recommender systems, Part 1. Introduction to approaches and algorithms. Learn about the concepts that underlie web recommendation engines. IBM. Available at: https://www.ibm.com/developerworks/opensource/library/os-recommender1/os-recommender1-pdf.pdf
21. Jia, Y., Zhang, C., Lu, Q., Wang, P. (2014). Users' brands preference based on SVD++ in recommender systems. 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA). doi: https://doi.org/10.1109/wartia.2014.6976489
22. Çano, E., Morisio, M. (2017). Hybrid recommender systems: A systematic literature review. Intelligent Data Analysis, 21 (6), 1487–1524. doi: https://doi.org/10.3233/ida-163209
23. Koren, Y. (2009). Collaborative filtering with temporal dynamics. Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '09. doi: https://doi.org/10.1145/1557019.1557072
24. Meleshko, Y., Raskin, L., Semenov, S., Sira, O. (2019). Methodology of probabilistic analysis of state dynamics of multi¬dimensional semi¬Markov dynamic systems. Eastern-European Journal of Enterprise Technologies, 6 (4 (102)), 6–13. doi: https://doi.org/10.15587/1729-4061.2019.184637