Development of the analyzing system for user’s actions in the informational environment

N E Karpova, A S Baranov, A A Emelina, A E Konovalov
Electronic Systems and Information Security Department, Samara State Technical University, 244 Molodogvardeyskaya street, Samara, 443001, Russia
E-mail: esib@samgtu.ru

Abstract. The main topic of the article is the analysis of user actions in a computer system and the development of a monitoring system for anomalous user actions in the information environment. To develop the system, the mathematical apparatus of fuzzy logic was used. The main advantage of information environment monitoring systems based on the theory of fuzzy sets is the ability to take into account most of the development scenarios while describing schemes for analysing flows of the information environment, as well as to track a large number of computer parameters. In the course of the study, it was revealed that the actions of intruders differ from the behaviour of ordinary users. As a result, the authors propose a developed system for monitoring anomalous user actions in the information environment, which is based on the analysis of event logs. A system operation requires an accumulation of information (audit files, data on login time and session duration, data on file deletion, etc.), on the basis of which a standard (template) of normal user behaviour is created. Then, the user's behaviour is compared with the standard, and when anomalies are detected, the system signals deviations. This algorithm makes it possible to track a large number of user parameters to determine unauthorised access.

1. Introduction
The majority of crimes related to information security are committed by companies’ employees. This is confirmed by a survey [1], according to which 90% of companies note their vulnerability to internal threats.
Currently, there is a significant number of systems that implement mechanisms for protecting information systems from both external and internal threats. Such systems include intrusion detection systems (IDS). They are divided into systems that respond to already known threats (attacks) - complex systems, and systems that monitor and analyse user actions in the system.
Monitoring systems allow identification and authentication of a user and analysis of his/her actions, including detecting anomalies in the behaviour. They are divided into behavioural and biometric. Behavioural systems make it possible to detect suspicious behaviour that does not correspond to the typical user actions in the system. Biometric systems allow users to be recognised by their physical individual characteristics (fingerprints, voice, hands, DNA, etc.) These systems are mainly used in access control and management systems, which allow an attacker, having gained access to the system, to freely use it for his/her own purposes.
Behavioural systems are more flexible than biometric ones and allow analysis of user actions in the information environment, also from the point of view of identifying previously unknown behaviour anomalies. Protection systems including monitoring systems based on behavioural analysis of user actions are quite common.
The main methods of monitoring user behaviour in the network are described in a number of scientific works [2,3,4,5]. For instance, in their work Averkin A. and Tarasov V. consider the irrationality of
human behaviour when making a decision [2]. Nikitin P., Savinov A., Bazhenov R. and Sivandaev S. describe methods, models and algorithms for recognising a keystroke pattern in key systems. He concludes that the most convenient way to ensure the procedure of constant covert analysis in order to detect operator substitution is the keystroke pattern. It is a dynamic behavioural biometric characteristic of a person [4]. These algorithms do not contain a description of the user identification and authentication mechanism in real time. In addition, the works omit other important user capabilities: the use of a computer mouse and the features of operating the system itself as a whole.

In the article [5], the analysis of methods for recognising the keystroke pattern is carried out on the basis of comparing the reference Gaussian values with the new received values. The scheme of statistical analyser of a keyboard pattern on the basis of standard Gaussian signals is presented and analysed. On the basis of the statistical analyser and the poly-Gaussian models and algorithms implemented in it, a system for recognising the user's keystroke pattern is being developed. Article [6] is about a development of a system analysing event logs in a critical industrial system. The results demonstrate that the proposed method is effective for storing interesting events with high accuracy. However, the flexibility of the system is initially under a question, since no testing is performed on different sets of security event data to be able to understand the limitations of the method under different conditions.

There are also systems tracking the features of working with a keyboard and a mouse. Article [7] proposes to introduce an additional user authentication based on the nature of the user's work with the mouse. However, the emotional state of users can have a profound effect on the behaviour of the mouse and thus cause an incorrect result. The influence of external factors, such as room temperature, is not known. Also, this approach is not comprehensive, thus, a high level of reliability of this method is not guaranteed.

In the article [8], attempts were made to improve the existing authentication methods using continuous active authentication methods based on modeling and checking the interaction between the user and the system, as well as using "false file systems". This approach is designed to detect unauthorised use of user credentials by periodically checking the behaviour against known profiles. However, this system has a number of disadvantages such as the need for constant readjustment of the program, sensors and staff training in case of high staff turnover. Its effectiveness has not been proven because pentesters and ordinary users of the system showed the same result of activating these traps.

The systems described above are based on mathematical models describing user actions. These models include models of decision-making with the involvement of experts based on the theory of probability; operational control models using mathematical statistics; models describing schemes and flows in an information system based on graph theory; models based on the use of fuzzy sets; methods of early detection of an internal violator of information security using Bayesian networks; systems based on neural networks [9, 10, 11, 12].

In most cases models based on the use of neural networks, Bayesian networks and fuzzy logic are used to construct monitoring systems for working methods in an information environment [10, 11, 12, 13]. Each type of a model has its own advantages and disadvantages.

The advantages of neural networks include effective filtering of noise, the ability to adapt to changes in input data, fault tolerance and high operating speed. One of the disadvantages of neural networks is that the problem of retraining can be noted, since a neural network is essentially a black box. This model has a certain feature that is called catastrophic forgetting [14]. Bayesian networks are quite easy to understand, they can combine regular patterns deduced from statistical data and expert knowledge obtained from real practice. Another advantage is the possibility of establishing connection between all variables in the model. But there are shortcomings such as the attention drawn to the impossibility of direct processing of continuous variables, the need to multiply conditional probabilities only if all input variables are really independent statistically. In the naive Bayesian approach, the result of classification is not affected by the combined value of pairs of different attributes [13].

The difficulties faced by the modelers are associated with the fact that all the methods mentioned above relate to the description of human behaviour, which is difficult to formalise [15]. Therefore, to describe the behavioural characteristics of a person, it is appropriate to use a mathematical apparatus
that makes it possible to display all the diversity and complexity of human behaviour. Fuzzy sets and fuzzy logic allow us to take into account the invariance of human behaviour, to describe specific user actions in the system and to take into an account the probability of unauthorised actions in the information environment. An important advantage of models of real systems built on the basis of fuzzy mathematics is their greater flexibility and adequacy to the real world, as well as, in comparison with traditional models, faster obtaining of the final result through the specific construction and simplicity of the fuzzy operations used.

Considering all the above, this article proposes the development of a system for analysing user actions in an information environment based on the use of the mathematical apparatus of fuzzy logic.

2. Research

In educational institutions there is a need to monitor the actions of users (students) in the information space and block them if they can harm the information system. Therefore, the detection of suspicious and anomalous (dangerous) user behaviour is an important and urgent task. By a suspicious and anomalous command, we mean user activity not related to educational tasks, which can damage the information resources of the university.

The Institute of Automation and Information Technologies at Samara State Technical University was chosen as an object for the research. Until now, this Institute has been solving the task with the help of preinstalled protection tools (Kaspersky Anti-Virus, Firewall operating system) and manual monitoring of user actions by the administrator. Despite the methods of protection used, not all malicious actions of users were timely detected and prevented in real time. This situation has led to the need to develop an automated system for monitoring and analysing the actions of users of the Institute's information system.

To develop such kind of a system, at the first stage, the behaviour of this system's users was studied implementing the mathematical apparatus of fuzzy logic and defining normal (safe), as well as suspicious and abnormal behaviour. At the second stage, fuzzy rules for this system's functioning were developed. At the third stage, the structure of the system for monitoring and analysing user actions in the information environment was developed and tested.

In this research, six information system's parameters of the Institute of Automation and Information Technologies at Samara State Technical University were analysed in order to determine normal, suspicious and abnormal user behaviour. These parameters include: the paths of users' movement in the system, duration of the session in the system, log in and log out times in the information system, extension of newly created files, frequently used programs, and file storage time. The study of these parameters allows for a comprehensive analysis of user actions and a timely response to anomalous actions in the system associated with unauthorized access. As part of the research, the event logs for one month were analysed in 50 educational computers located in the university classrooms.

The main users of the computers were students of this university. The analysis was carried out using the method of expert assessment and the method of relative frequencies (direct group method). As experts, 11 people were involved, who are teachers and system administrators at this Institute.

When analysing the selected parameters, their membership functions were determined. In the general case, the degree of membership \( \mu_A(x) \) is some non-probabilistic subjective measure of fuzziness, determined as a result of surveying experts about the degree of the correspondence of an element \( x \) to a concept formalized by a fuzzy set \( A \). Thus, the membership function \( \mu_A(x) \in [0.1] \) puts in accordance with each number \( x \in X \), a number from the interval \([0.1]\) characterising the degree of a membership of the solution in the subset \( A \).

When analysing the parameter “User movement paths in the system”, a fuzzy set \( A \) was formed, corresponding to the concept of “user movement path in the system is safe”. 13 main paths of movement were identified and a set \( X \) was formed - a set of paths for the user's movement, where objects \( x_i \) are specific paths that the user visits while working in the system (table 1).

To determine whether the use of each specific path is normal or suspicious behaviour, the experts were presented with different names of the user's paths in the system \( x_i \) and each of them was asked the following question: with what degree of a confidence \( 0 \leq \mu_A(x) \leq 1 \) does the expert believe that this user’s movement path in the system is safe. The results of expert assessments are shown in table 2.
Table 1. The list of main paths in the system

| x | Path                                      |
|---|-------------------------------------------|
| 1 | "C:\Windows\Logs"                       |
| 2 | "C:\Windows\System32"                   |
| 3 | "C:\Windows\"                            |
| 4 | "C:\Program Files"                      |
| 5 | "C:\Users\\Documents\Downloads\"       |
| 6 | "C:\Documents and Settings\student\desktop" |
| 7 | "C:\Documents and Settings\student\My document" |
| 8 | "C:\Users\\Documents\"                  |
| 9 | "C:\Documents and Settings\student\"     |
| 10| "C:\Users\"                              |
| 11| "C:\Users\"                              |
| 12| "C:\Documents and Settings\"             |
| 13| "C:\"                                    |

Based on the experts' answers using the method of relative frequencies (1), $\mu_A(x)$ was calculated.

$$\mu_A(x) = \frac{n_1}{n_1 + n_2} = \frac{n_1}{m},$$

where $m$ is the total number of experts, $n_1$ are experts who answered positively to the question of whether an element $x_i \in X$ belongs to a fuzzy set $A$, $n_2 = m-n_1$ are experts who answered this question negatively. Calculation results are also shown in table 2.

Table 2. Experts’ assessment results

| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|
| $n_1$ | 2 | 2 | 3 | 7 | 6 | 7 | 7 | 8 | 8 | 9  | 10 | 10 | 11 |
| $n_2$ | 9 | 9 | 8 | 4 | 5 | 4 | 4 | 3 | 3 | 2  | 1  | 1  | 0  |
| $\mu_A(x)$ | 0.2 | 0.2 | 0.3 | 0.6 | 0.6 | 0.6 | 0.7 | 0.7 | 0.8 | 0.9 | 0.9 | 1.0 |

Based on the data in table 2, the membership function in analytical (2) and graphical form is constructed (figure 1).

Figure 1. A graphical representation of the membership function of user access to folders and files.
In figure 1 it can be seen that the anomalous user’s behaviour is visiting system folders, as well as folders that do not correspond to educational tasks, which corresponds to the condition $\mu_A(x) \leq 0.4$. Suspicious behaviour will be defined as behaviour for which $0.4 < \mu_A(x) \leq 0.6$.

The next parameter selected for analysis is the logon and logoff times. The time intervals for the analysis were selected based on the duration of the classes and the working hours of the university. Logging in to the system occurs more often in the morning. It also takes into account the break at lunchtime. In the afternoon, classes are also held, but there are fewer of them, and, consequently, the number of users working in the system is less at this time. At 18.40 the last classes end, so after this time there should be no actions to enter and exit the system. Also, when analysing this parameter of the information system, it should be taken into account whether the day under analysis is a weekday or a weekend. At 7 pm the information system automatically blocks the switched on computers.

When analysing the parameter "Time of the entry and exit from the information system", a fuzzy set $B$ was formed, corresponding to the concept of "the time interval for the beginning and the end of the user's session is safe". Five main time intervals for the beginning and the end of the session have been determined and a set $T$ is formulated, that is the set of time intervals for the beginning and the end of the session, where objects $t_i$ are the time intervals in which the user visits the system (table 3).

To determine whether the time interval of the beginning and the end of the session is normal or suspicious behaviour, the experts were presented with different time ranges of the user's entry and exit from the system $t_i$ and each of them was asked the following question: with what degree of confidence $0 \leq \mu_B(t) \leq 1$ does the expert consider that the given time interval marking the beginning and the end of the user's session, is safe. The results of the survey are summarized in table 4.

### Table 3. Log in and log out times.

| $t_i$ | Time (min) |
|-------|-------------|
| $t_1$ | 07.55–13.15 |
| $t_2$ | 13.15–13.30 |
| $t_3$ | 13.30–15.20 |
| $t_4$ | 15.20–18.40 |
| $t_5$ | 18.40–07.55 |

Based on the experts' answers using the method of relative frequencies (3), $\mu_B(x)$ was calculated.
where \( m \) is the total number of experts, \( n_1 \) are experts who answered positively to the question of whether an element \( t_i \in T \) belongs to a fuzzy set \( B \), \( n_2 = m - n_1 \) are experts who answered this question negatively.

Calculation results are also shown in table 4.

**Table 4.** Experts’ assessment results.

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| \( n_1 \) | 2 | 7 | 9 | 4 | 9 |
| \( n_2 \) | 9 | 4 | 2 | 7 | 2 |
| \( \mu_B(t) \) | 0.2 | 0.6 | 0.8 | 0.4 | 0.8 |

Based on the data in table 4, the membership function is constructed in the analytical (4) and graphical form (figure 2).

\[
\mu_B(t) = \frac{n_1}{n_1 + n_2} = \frac{n_1}{m},
\]

\[
(3)
\]

\[
\mu_B(x) = \begin{cases} 
  t_1, 0.8; \\
  t_2, 0.4; \\
  t_3, 0.8; \\
  t_4, 0.6; \\
  t_5, 0.2. 
\end{cases}
\]

(4)

**Figure 2.** A graphical representation of the membership function of entry and exit times.

Figure 2 shows that behaviour for which \( \mu_B(t) \leq 0.4 \) can be considered as anomalous. Two variants of abnormal behaviour can be noted: working during lunchtime \( (t_2) \) and sessions of working in the information system out of working hours. Suspicious behaviour is considered to be behaviour for which \( 0.4 < \mu_B(t) \leq 0.6 \).

The next parameter of the information system related to the creation of files is to be considered. As it was mentioned above, the main users of the information system are students of the Institute of Automation and Information Technology, who use computers to perform practical and laboratory works. When creating files, students use standard extensions, namely: text (*.txt, *.docx, *.pdf and others), graphic (*.gif, *.jpeg, *.png, *.tif and others), archive (*.zip, *.rar and others), web pages (*.html, *.xml and others), executable files (*.exe and *.com). In addition, in connection with the use of special software, the following file formats are used: nanoCAD (*.dwg), IP Video System Design
Tool (*.jvsg), and Multisim (*.mc8). Creation of files with other extensions, for example, executable files (*.pif, *.scr and others), scripts (*.bat, *.cmd, *.vbe and others), shortcuts (*.scf, *.lnk, *.inf and others), register files (*.reg), may indicate anomalous behaviour, and the files themselves may be potentially dangerous. For example, a specially or accidentally created *.reg file at startup can delete important registry information or modify it, which can lead to system errors and also create a vulnerability through which attackers gain access to the information system of the Institute.

When analysing the "Extension for newly created files" parameter, a fuzzy set \( C \) was formed, corresponding to the concept of "a file created with this extension is safe". 12 main file extensions were identified and a set \( N \) was formed - a set of file extensions that the user can create while working in the system, \( n_i \) objects are files with extensions that can be created by the user while working in the system (table 5).

To determine whether the extension of newly created files is normal or suspicious, the experts were presented with different names of file extensions \( n_i \) created by the user while working in the system, and each of them was asked the following question: with what degree of confidence \( 0 \leq \mu_C(n) \leq 1 \) does the expert believe that the file created with this extension is safe. The results of the survey are summarised in table 6.

| \( n_i \) | File type              |
|---------|-----------------------|
| 1       | script                |
| 2       | register              |
| 3       | Shortcut              |
| 4       | executable            |
| 5       | executable (.exe, .com) |
| 6       | archive               |
| 7       | nanoCAD               |
| 8       | IP Video System Design Tool |
| 9       | Web-page              |
| 10      | Multisim              |
| 11      | text                  |
| 12      | graphic               |

Based on the experts' answers using the method of relative frequencies (5), \( \mu_C(n) \) was calculated.

\[
\mu_C(n) = \frac{n_1}{n_1 + n_2} = \frac{n_1}{m},
\]

where \( m \) is the total number of experts, \( n_1 \) are experts who answered positively to the question of whether an element \( n_i \in T \) belongs to a fuzzy set \( C \), \( n_2 = m - n_1 \) are experts who answered this question negatively.

Calculation results are also shown in table 6.

| \( n \) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|-------|---|---|---|---|---|---|---|---|---|----|----|----|
| \( n_1 \) | 1 | 2 | 3 | 3 | 5 | 5 | 5 | 8 | 8 | 8  | 10 | 10 |
| \( n_2 \) | 10| 9 | 8 | 8 | 6 | 6 | 6 | 3 | 3 | 1  | 1  | 1  |
| \( \mu_C(n) \) | 0.1| 0.2| 0.3| 0.3| 0.5| 0.5| 0.5| 0.7| 0.7| 0.7 | 0.9 | 0.9 |

Based on the data in table 6, the membership function is constructed in the analytical (6) and graphical form (figure 3).
Figure 3. A graphical representation of the membership function of assigning an extension to newly created files.

From the data presented in figure 3, it can be seen that anomalous behaviour will be the creation of all types of executable files, except *.com and *.exe, as well as register and script files and file shortcuts, which corresponds to the condition $\mu_D(t) \leq 0.4$. Suspicious behaviour is considered to be behaviour for which $0.4 < \mu_C(n) < 0.5$.

The analysis of the following three parameters was carried out in a similar way: the duration of the computer operation, the analysis of the list of frequently of the programs used, and the duration of a file storage. For the above parameters, membership functions were determined in an analytical and graphical forms and it was shown that an abnormal duration of work at a computer is a work over 4.5 hours (which corresponds to the condition $\mu_D(t) \leq 0.4$). Suspicious behaviour for this parameter will be the running time for which $0.4 < \mu_C(t) \leq 0.6$. Likewise, using programs for which $\mu_E(x) \leq 0.4$ will be considered as anomalous behaviour as these programs should not be used by students. The use of programs for which $0.4 < \mu_E(x) < 0.5$ will be considered as suspicious behaviour for this parameter. For the "File storage duration" parameter, the normal storage duration is 1.5 - 3 hours, so during this time the student has enough time to complete the assigned task. Any other storage durations, for which $\mu_F(t) \leq 0.4$ is considered to be anomalous, since in this case the files are stored longer than it is necessary to perform laboratory and practical work. Suspicious behaviour for this parameter will be such a file storage time at which $0.4 < \mu_F(t) \leq 0.7$. 

\[
\mu_C(x) = \begin{cases} 
  n_1, 0.1; \\
  n_2, 0.2; \\
  n_3, 0.3; \\
  n_4, 0.3; \\
  n_5, 0.5; \\
  n_6, 0.5; \\
  n_7, 0.5; \\
  n_8, 0.7; \\
  n_9, 0.7; \\
  n_{10}, 0.7; \\
  n_{11}, 0.9; \\
  n_{12}, 0.9. 
\end{cases} 
\]
2.1 Results Analysis
Based on the membership functions for each parameter, the boundaries of normal, suspicious and abnormal user behaviour in the information environment are defined. The results are shown in table 7.

| Parameter                          | normal      | suspicious   | abnormal    |
|------------------------------------|-------------|--------------|-------------|
| Usage of folders                   | 0.6<μ_A(x)  | 0.4<μ_A(x)≤0.6 | μ_A(x)≤0.4  |
| Log in and log out times in the information system | 0.6<μ_B(t)  | 0.4<μ_B(t)≤0.6 | μ_B(t)≤0.4  |
| Extension of newly created files   | 0.5≤μ_C(n)  | 0.4<μ_C(n)<0.5 | μ_C(n)≤0.4  |
| Session duration                   | 0.6<μ_D(t)  | 0.4<μ_D(t)≤0.6 | μ_D(t)≤0.4  |
| Frequently used programs           | 0.5≤μ_E(x)  | 0.4<μ_E(x)<0.5 | μ_E(x)≤0.4  |
| File storage time                  | 0.7<μ_F(t)  | 0.4<μ_F(t)≤0.7 | μ_F(t)≤0.4  |

Based on the data obtained, the following conclusions can be drawn.

The behaviour of a user (student) is normal if he/she performs the following actions:
– enters the information environment only during classes with a duration of work in the system of no more than 4.5 hours;
– uses in his work only educational programs, such as: Visual Studio, IDAPro, IP Video System design Tool, Microsoft Office, NanoCad, Multisim;
– creates the following types of files: text, graphic, .dwg, .jvsg, .mc8;
– deletes only those files that he himself created.

Actions other than the reference behaviour will be considered as suspicious or abnormal and will require notification of the administrator, detailed examination of user actions and blocking the user if necessary to prevent unauthorised actions.

In addition, based on the data obtained, it can be stated that if the files used are abnormal, then the folder in which they are located is also rarely used; if a program from the list of "abnormal" programs is used, the extension of the created file is also abnormal; if a file is stored for longer than the normal duration and files are deleted outside of the normal session, this behaviour is also considered as abnormal.

1. If <folder usage - abnormal> or <session duration - abnormal> or <time of entry and exit from the information system - abnormal> or <extension of newly created files - abnormal> or <frequently used programs - abnormal> or <file storage time - abnormal>, then <blocking user actions>.

2. If <folder usage - suspicious> or <session duration - suspicious> or <time of entry and exit from the information system - suspicious> or <extension of newly created files - suspicious> or <frequently used programs - suspicious> or <storage time files - suspicious>, then <informing the administrator>.

3. If <folder usage - normal> and <session duration - normal> and <time of entry and exit from the information system - normal> and <extension for newly created files - normal> and <frequently used programs - normal> and <file storage time - normal>, then <no action required>.

3. Practical Implementation
Based on the data obtained, the formulated fuzzy rules and the user's standard, the system for analysing anomalous user actions in the information environment was developed. Its structural diagram is shown in figure 4.
Figure 4. A block diagram of a system for analyzing user actions in the information environment.

Operations of the system require accumulation of data, on the basis of which a standard of normal user behaviour is created. Then the system compares the user's behaviour with the standard according to six defined parameters, such as: the paths of users' movement in the system, duration of the session in the system, log in and log out times in the information system, extension of newly created files, frequently used programs, and file storage time. When anomalies or suspicious behaviour are detected, the system signals deviations and, if necessary, blocks the user.

The system for analysing anomalous user actions in the information environment is developed in the C# language. It was tested in the classrooms of the Institute. The system has shown itself to be a stably functioning application that makes it possible to detect all cases of suspicious and abnormal behaviour described above. The advantages of the system include the detection and prevention of malicious user actions in real time.

4. Conclusion

Thus, the article presents a system for analysing anomalous user actions in the information environment of the Institute of Automation and Information Technologies at Samara State Technical University. The system was developed using the apparatus of fuzzy logic.

The system being developed has a number of advantages over existing analogs. Firstly, this system does not put a lot of load on the resources of the local network, and it requires minimal technical characteristics from the computers on which it will be installed. Secondly, working with this monitoring system does not require additional trainings, and it will be accessible and understandable to the user and the system administrator. Thirdly, the cost of the system under development is much lower than the products available on the market for detecting anomalous user actions.

5. References

[1] Seals T 2017 Fear of Insider Threats Hits an All-Time High Infosecurity Magazine Retrieved
[2] Averkin A and Tarasov V 1987 The fuzzy modelling relation and its application in psychology and artificial intelligence Fuzzy sets and systems 22(1-2) 3–24
[3] Ramani A and Dewangan S 2014 Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device Int. Journal of Computer Science and Information Technologies 5(2) 1045–52
[4] Nikitin P, Savinov A, Bazhenov R and Sivandaev S 2018 Algorithm for personal identification in distance learning system based on registration of keyboard rhythm Journal of Physics:
Conference Series Int. Conf. Information Technologies in Business and Industry 2018 p 042043

[5] Sharipov R, Tumbinskaya M and Abzalov A. 2019 Analysis of users' keyboard handwriting based on gaussian reference signals Proceedings - 2019 international russian automation conference, rusautocon (New York:IEEE) p 886753

[6] Cinque M, Della Corte R and Pecchia A 2019 Contextual filtering and prioritization of computer application logs for security situational awareness. Future Generation Computer Systems 111 668-80

[7] Qian Y, Shiquan X, Biao W and Shuping Y 2020 Identification of trusted interactive behavior based on mouse behavior considering web User's emotions International Journal of Industrial Ergonomics 76 102903

[8] Jonathan V, Yingbo S, Salem M B, Shlomo H and Salvatore S 2019 Active authentication using file system decoys and user behavior modeling: results of a large scale study. Computers & Security 87 101412

[9] Lozano C et al. 1997 Neural Networks for System Security. Proc. Of 5th European Congress on Intelligent Techniques and Soft Computing (Aachen, Germany) vol 1 pp 410–14

[10] Obaidat M and Macchairolo D 1994 A multilayer neural network system for computer access security. EEE Trans. on Syst., Man, and Cybern. 24(5) 806–13

[11] Domanetska I, Khaddad A, Krasovska H and Yeremenko B 2019 Corporate system users identification by the keyboard handwriting based on neural networks Int. journal of innovative technology and exploring engineering 9(1) pp 4156–61

[12] Hodo E et al. 2016 Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System 2016 Int. Symposium on Networks, Computers and Communications (ISNCC) (New York: IEEE) pp 1–6

[13] Zvyagin L 2017 Iterative and non-iterative methods of Monte Carlo as actual computing methods Bayesian analysis Proceedings of 2017 XX IEEE international conference on soft computing and measurements (SCM) (New York: IEEE) pp 18–21

[14] Zhou Z-H 2004 Rule Extraction Using Neural Networks or For Neural Networks? Journal of Computer Science & Technology 19(2) 249–253

[15] Karpova N and Panfilova I 2019 Ensuring the Safety of Information Processes in Sociotechnical Systems Based on an Analysis of the Behavioral Characteristics of a Person as a Subject of Such a System 2019 XXI Int. Conf. Complex Systems: Control and Modeling Problems (CSCMP) (New York: IEEE) pp 751–53