Journal of Theoretical and Applied Information Technology
15th February 2022. Vol.100. No 3
© 2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DECENTRALIZED APPROACH FOR COLLECTING AND PROCESSING DATA OF THE ENTERPRISE INFORMATION INFRASTRUCTURE

[1]E.A.BASINYA, [2]G.T.MERZADINOVA, [2]A.B.ZAKIROVA, [2]ZH.B.AKHAYEVA, [2]G.TOLEGENOVA, [2]A.K.ALZHANOV, [2]M.A.KANTUREYEVA, [2]A.ZH.AKHMETOVA

[1] Novosibirsk State Technical University, Department of Automation, Novosibirsk, Russia
[2] L.N.Gumilyov Eurasian National University, Department of Information Systems, Astana, Kazakhstan

E-mail: [1]basinya@mail.ru, [2]merzadinova_gt@enu..kz, [2]alma_zakirova@mail.ru, [2]ahaeva07@mail.ru, [2]gulnaztolegenova@mail.ru, [2]alzhanov_ak@mail.ru, [2]ma_khantore@mail.ru, [2]akhmetova_azh@mail.ru

ABSTRACT

The level of security of the information and communication sector of an enterprise is a consequence of the effectiveness of solving problems of system analysis, management and processing of information in a corporate computer network. The article analyzes the problem of responding to incidents in cyberspace on the basis of existing centralized and distributed systems for collecting and analyzing events. Threats of unauthorized influences from trusted users are considered. An original method of system analysis, management and information processing of a corporate computer network is presented for review. The scientific novelty of the proposed solution lies in the ability to automatically control the traffic of a computer network and local information processes of its hosts based on an objective and informative register of events, protected from various external disturbances (from impersonation attacks to falsification of records) by using a modified decentralized blockchain storage with a trust management system to logged events.

Keywords: *System Analysis, Management, Processing, Logs, Blockchain Storage, Trust Management, Multilayer Encapsulation.*

1. INTRODUCTION

Cybersecurity advocates as one of the key factors in the development of the national security strategy of the Russian Federation, affecting all spheres of society: from economic to social and political. The international community is developing various cybersecurity strategies designed to ensure the secure, reliable and resilient functioning of the cyberspace infrastructure with automatic control over emerging risks. Unfortunately, transnational cooperation in this area has been undermined by mutual accusations of various states and manufacturers of information and communication solutions in industrial espionage and political engagement. An example is the conflict between the United States of America and Huawei. Accordingly, the trend of development of our own proprietary systems for protecting critical national infrastructure is growing.

In order to effectively respond to incidents in cyberspace, scientists are developing various algorithms and methods for the operation of intrusion detection and prevention systems. Original approaches in the field of identification of network anomalies and parallelization based on embedded microprocessor systems described in the works of A.S. Bondyakov, A.Yu. Efimov, S.M. Dotsenko, A.G. Vladyko, I.D. Letenko. [1-3]. Another concept is the use of machine learning and the development of automatic penetration testing into such classes of systems, described in the works of P.R. Chandre, P.N. Mahalle, G.R. Shinde, T. Zitta, M. Neruda, L. Vojtech, M. Matejkova [4–6]. Unfortunately, these systems are not focused on functioning in real infrastructures, where technologies of virtual secure communication channels and encryption protocols are used.

The existing algorithms, methods and approaches are based on standard primary information collection agents: syslog system log in

Linux/Unix operating systems, evtx event log in Windows operating systems. But these logs are not exhaustively informative. As an example, it is worth mentioning continuous remote work using the RDP protocol for an hour, when on a remote machine in the evtx event log, instead of two entries for the types of events of interest, more than 80 entries with log in log out types are formed, despite the continuous nature of the work. Accordingly, the investigation of cybercrimes will require additional sources and mechanisms (up to the analysis of temporary files and memory dump). Another significant disadvantage of best practices is the lack of verification of trust in the recorded information. The potential possibility of registering deliberately false information is not considered. This approach does not take into account insider attacks (malicious actions of trusted users), as well as impersonation attacks. It is worth noting that even the basic protocols of the TCP/IP stack and operating system mechanisms do not include authentication of the subject of interaction and metadata during communication.

Thus, the problem statement is formulated as follows: existing solutions in the field of primary collection and processing of information about the events of the information infrastructure of the enterprise have low informativeness, do not verify the authenticity of the recorded information, while introducing significant redundancy. The consequence is the absence of global observability, a decrease in the effectiveness of monitoring and management of objects of corporate computing networks in conditions of a shortage of reliable initial conditions.

Accordingly, the relevance of the development of methods for complex collection and processing of data with the ability to verify their authenticity and reliability is increasing.

The purpose of this work was to develop an original method for system analysis, management and information processing of a corporate computing network operating on the basis of the TCP / IP protocol stack.

The scientific novelty of the proposed solution lies in the possibility of automatic traffic control of a computer network and local information processes of its hosts based on an objective and informative register of events protected from various external disturbances (from impersonation attacks to falsification of records) by using a modified a decentralized blockchain storage with a trust management system for registered events.

The limitation of the study lies in the permissible initial values and parameters of the object and subject of the study. The object of research is managed hardware and software hosts of the enterprise information infrastructure. The subject of the study is the traffic of computational networks operating on the basis of the TCP/IP protocol stack versions 4 and 6, and information processes of operating systems of the Linux, Windows, Mac OS family.

The functioning of managed technical objects and systems is carried out on the basis of client and server operating systems of the Linux family (rpm-oriented versions of Red Hat Linux 8 and 9, CentOS from v5 to v8, Fedora from v8 to v34 and their derived assemblies; deb-oriented versions of Debian from 4.0 <Etch> to 11 <Bullseye>, Ubuntu from 7.04 <Feisty Fawn> to 21.04 <Hirsute Hippo> and their derived assemblies, as well as Alpine Linux from v2.1 to v3.14 and many other versions) and Windows (Windows 7, 8, 8.1, 10, 11, Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2022). An optional (auxiliary, optional) requirement is Mac OS support (Leopard 10.5.8, Snow Leopard 10.6.8, Lion 10.7.5, Mountain Lion 10.8.5, Mavericks 10.9.5, Yosemite 10.10.5, El Capitan 10.11.6, Sierra 10.12.6, High Sierra 10.13.6, Mojave 10.14.6, Catalina 10.15.7, Big Sur 11.5.2, Monterey 12).

The developed method is an integral part of the author's complex methodology of intellectual and adaptive management of the information infrastructure of the enterprise. The methodology and the system functioning on its basis should carry out comprehensive monitoring and management of all objects of the enterprise's information infrastructure: managed network equipment (switches, routers and other objects), user electronic computers, dedicated and virtual servers, managed network equipment, proprietary knowledge-intensive systems, technical facilities and industrial systems (including components of automated process control systems).

The proposed methodology and system should function at all levels of the TCP/IP protocol stack, comply with the standards of the IEEE protocols and technologies used, comply with the requirements of RFC 791, RFC 2474, RFC 3168, RFC 793/STD 7, RFC 768/STD 6 and a number of other governing documents, specifications and industry standards.

It is necessary to provide support for various channel layer technologies, including IEEE 802.3 Ethernet packet data transmission technology (100BASE-TX, 100BASE-T4, 100BASE-FX,

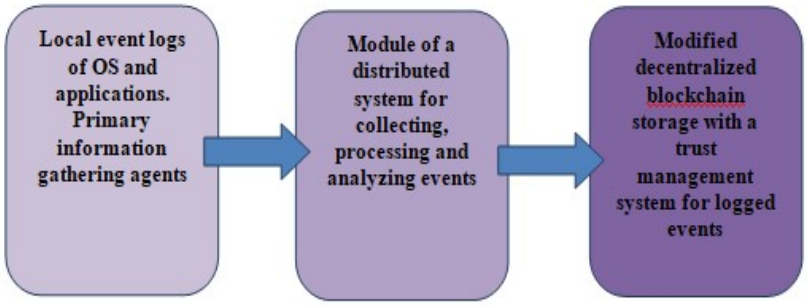
10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW, 10GBASE-CX4, 10G-EPON, 10GPASS-XR, 1000BASE-T1, 100G-EPON, 10BASE-T1L and many others)..

2. ORGANIZATION OF AUTOMATIC TRAFFIC CONTROL FOR COMPUTING

To level the previously described threats, an original method of system analysis, management and processing of information of a corporate computer network using a modified decentralized blockchain storage and an author's system for managing the trust to registered events submitted for review. The purpose of this approach is to organize automatic traffic control of a computer network and local information processes of its hosts based on an objective and informative register of events, protected from various external disturbances: from impersonation attacks to falsification of records.

The objectivity of an event implies the transparent provability of the fact of its existence, combined with ensuring the confidentiality, integrity and authenticity of the data.

The informativeness of events is achieving by using the author's distributed system for collecting, processing and analyzing events of the enterprise network infrastructure. Above the standard agents of primary collection of information (event logs of the operating system, applications, network traffic, etc.), an abstraction layer is introduced in the form of the system module of the same name (Fig. 1).



Object / Host Of Corporate Computer Network

Fig. 1. The Sequence Of Identification And Processing Of Events On The Host.

The module under index 2 performs not only parsing, but also identification, structuring, ranking, combining events with the identification of correlation. This allows you to significantly reduce the amount of data, unify their format for all operating systems, and increase information content. Its functioning is carried out on the basis of the original signature and statistical method of compiling the knowledge base of the system by testing and simulating known network and local disturbances with tracking the response of operating systems and applications in a virtualization environment. An automated investigation of correlated events is carried out with the use of deep analysis of the contents of packets and monitoring of the local work of users [7, 8].

This software package is subject to mandatory installation on gateway hosts (routers, switches, gateways and other objects integrated with the system of intelligently adaptive management of the enterprise network infrastructure). Installation on client computers is desirable but not required. The integration decision based on an estimate of the free disk space for the system and the capacity of the client computer.

Let us consider the proposed approach to the construction of a modified de-centralized blockchain storage of the register of events (logs) with a trust management system for the registered information on a simplified schematic diagram of a corporate computer network, shown in Fig. 2.

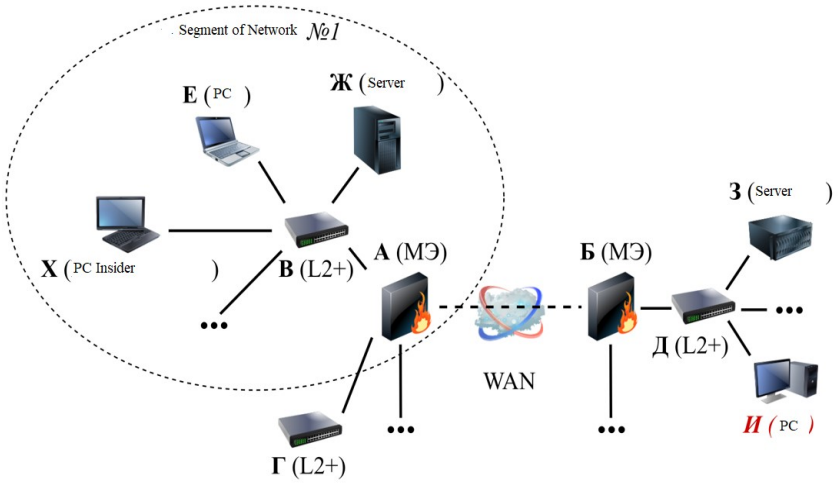


Fig. 2. Schematic Diagram Of A Corporate Computer Network.

The following objects function on the presented diagram:

 complex firewalls "A" and "Б", interacting on the basis of a virtual secure communication channel in the global Internet;

 Managed network switches "B", "Г", "Д", postfix L2 + reflects their partial operation at the higher levels of the OSI open systems interconnection basic reference model. A number of devices from different manufacturers allow their configuration via the HTTPS protocol (English Hy-perText Transfer Protocol Secure), but this does not mean the inclusion of full-fledged functionality up to the application level;

 various server solutions "Ф", "З";

 personal (corporate) computers based on various operating systems "E", "И", "X".

Hosts (objects, nodes, nodes) "A", "Б", "B", "Г", "Д", "Ж", "З", "E" are connected to a modified decentralized blockchain storage with the system trust management to the event registry (hereinafter simply the System), the computer "AND" is in the connection mode. Electronic computing device "X" is not connected to the system; it was accessed by an attacker from among the trusted persons.

All clients of the blockchain storage are equal regardless of the pre-purpose of the host system, the services running on it, and its computing resources. The exchange between the clients of the system is carried out via an encrypted communication channel. At the moment of transferring the logs of any host (hereinafter log), the rest of the network participants check the legality of the occurrence of this event. Each of the participants, after checking the legality / evidence of the event, exposes him his own coefficient of confidence, at the same time. After that, all participants sign the developed coefficients with their digital signature. In the blockchain storage, a log file is recorded, encrypted by the host generating this event, as well as all event assessments (even with negative confidence coefficients) generated by the participants of the System. Confidence factors are used to analyze network performance and identify unauthorized external disturbances.

As an example, it is worth mentioning various attacks using broadcast requests from insider "X". These unauthorized disturbances are produced and are transparent in network segment # 1, since the managed network switch "B" does not block broadcasts, and all network traffic from this device is duplicated onto the complex firewall "A" by port mirroring technology. Node "E" was the first to register the attack and initiated the transmission of the event to other hosts to check and assess the reliability of the information. All hosts of a given network segment can check the fact of such an event by means of primary information gathering agents and a module of a distributed system for collecting, processing and analyzing events in the enterprise network infrastructure. Objects "A", "B", "Ж", "E" confirm the event by setting trust coefficients "1" to it, and then the log file is safely written to the knowledge base (blockchain storage).

Thus, verification is carried out, verification of the objectivity, information content and authenticity of the event that has occurred, based on which it is possible to automatically control the traffic of the computer network and the local information processes of its hosts using specialized security tools. Further, it is necessary to

consider in detail the individual components of the System.

3. STORAGE AND PROCESSING SYSTEM OF LOGS

Information about events in the network infrastructure of an enterprise may be of interest to attackers as a set of initial information for preparing an attack; the decision to keep all logs in clear text is unacceptable. However, keeping data completely encrypted makes it harder to find it. As a compromise, it was decided to store the body of the log record in encrypted form, and use keywords that are stored in clear text for search. In this case, keywords can be used to prefetch data. The search itself is carried out in three stages:

1) Primary search of pre-election data by keywords;
2) Decoding the log of the electoral data body;
3) An accurate search for the decoded data.

After the third stage, the output will be data that fully corresponds to the search query. Note that this approach achieves multiple acceleration of the search by saving time to decrypt a large amount of information.

A balance must be struck between descriptive accuracy and information disclosure by publishing keywords in clear text. For example, keywords such as "06/19/2019 15:47:23 192.168.2.3:9999 FTP server start" can reveal information that at the specified time on the specified IP address on the non-standard port 9999 the FTP server started working ... This may well be sufficient for the initial drawing up of a strategy of unauthorized impact on the object. It is proposed to use as keywords: date and time of the event, the name of the service that generates the log record (event). In this case, the record cell will look like this (Fig. 3).

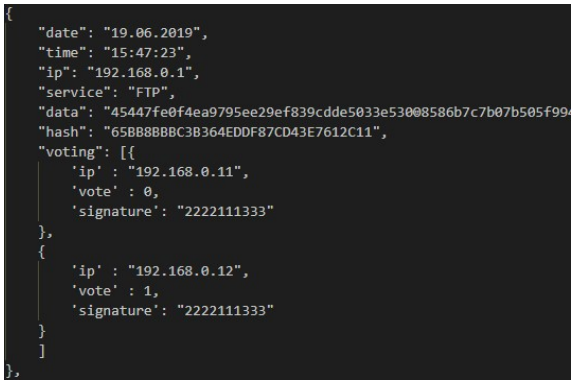


Fig. 3. An Example Of Data Writing To The Blockchain Storage.

It is important to note that a simplified example of data for writing to a blockchain storage is provided. Formalization and unification of record types is organized by the signature approach for various types of events.

4. TRUST MANAGEMENT SYSTEM FOR REGISTERED INFORMATION

One of the key differences of the proposed method is the introduction of a trust management system for the information being logged, using the trust coefficients of the log message. In this case, before any log is written to the blockchain storage, it is offered to be checked by the system's clients. Let us consider again using the example of a schematic diagram of a corporate computer network shown in Fig. 2. Client "Ж" offers to check a message about making a broadcast request to receive a pool of TCP / IP v4 stack settings by node "X" via DHCP v4 (Dynamic Host Configuration Protocol). The insider behind host "X" set a goal to disable the static settings of the network interface and initiate dynamic configuration. The rest of the network clients are trying to find information in their access to confirm or deny this event through the agents of the primary collection of information and the module of the distributed system for collecting, processing and analyzing events of the enterprise network infrastructure.

In total, there are three possible actions for the checking host:

1) the host can confirm the fact of the event occurrence: "+1";
2) the host can deny the fact of the event occurrence: "-1";
3) the host can neither confirm nor deny the fact of occurrence of the event: "0".

In this case, each of the reviewers assigns a rating to the message: "+1", "-1" or "0", respectively, and signs it with his digital signature. In the presented example, the actions of the node "X" are transparent for the network segment # 1. Accordingly, objects "A", "B", "Ж", "E" again confirm the event by setting the confidence coefficients "1" to it.

The rest of the hosts that are outside the considered network interaction can neither confirm nor deny the fact of the occurrence of the event and give a score of "0". Next, a secure log file is written to the knowledge base (blockchain storage).

In the future, the system for detecting and preventing intrusions in managing information flows and processes based on a decentralized

register of events will analyze the trust rating taking into account the segmentation of incidents.

5. SECURE LOCAL AND NETWORK COMMUNICATION SYSTEM

For connecting to the system, the host must generate private and public keys, and then generate a self-signed certificate based on them. The system does not use a single certification authority for signing certification requests, since such centralization would introduce additional security risks for corporate resources. The certificate is used to match the signature of trust coefficients when analyzing logs, as well as to organize secure group interaction of hosts in critical situations.

After generating keys and certificates, the host connects to the system. In this case, the System, taking into account the presence of a new exchange participant, generates a session key to encrypt the data exchange channel between the participants. To generate a session key, the Diff-fi-Hellman algorithm is used for an unlimited number of participants. In this case, if the host is disconnected, a new session key is generated, similar to the case of connecting a new host.

Each of the participants encrypts the old session key with their own public key and makes a record about it in the blockchain storage. This is necessary to restore all session keys and decrypt all log messages in the storage by all clients of the System. Further, all hosts publish their public key certificates to the blockchain storage. The decentralized event registry data is encrypted with a symmetric cryptographic key generated from the current session key.

After an event has occurred that led to the generation of a log message, the System node follows the algorithm:
1) generates keywords based on log messages;
2) gets a hash of log messages;
3) encrypts the log message using the session key;
4) sends a message to the blockchain network.

Each of the network participants, using the same session key, decrypts the message and sets the trust coefficient to it. After all the marks have been set, the log record, along with all the marks, will be written to the blockchain storage.

Intermediate saving of the session key in the system is necessary so that at any time, each of the participants can decrypt all their logs. In doing so, two important policies are followed:
1) any of the new members has access to all logs of all members of the System from the moment he was added to the network (with the exception of private records). Decryption of earlier System logs is impossible for him;
2) any of the remote network participants can read the logs only until the moment of their deletion. Decryption of later logs is impossible for him.

Since in existing systems, network reconfiguration with the removal or addition of new nodes is rare, it is proposed to artificially generate the procedure for creating a new session in short time intervals (every 30 minutes). This parameter is configured optionally during integration. Even if an attacker obtains a session key, he will be able to de-encrypt the logs only for a short period of time, within which confidential information of critical infrastructure objects of the enterprise will not be disclosed.

6. MAKING PRIVATE RECORDS

With this approach, in order for the system participants to assess the trust of the log message, that is, to confirm or deny the log event, all its participants must read all log events sent to the system. If in this case confidential information of critical infrastructure objects can be disclosed, a symmetric cryptographic key generated based on the session key and the user's private key can be used to encrypt the body of the log message. In this case, the message is marked as private: "public = False" and the trust coefficient will not be set, since the rest of the system participants will not be able to decrypt it.

This approach is used to write private data that is not subject to disclosure - the host from which they were written to the blockchain storage can only read them. Since the score cannot be set due to the lack of confirmation of the identity of the log message that the client wants to write to the blockchain in encrypted public key form, and the log message that the client sent to certain nodes of the System.

At the same time, the publication by all System participants of their public key certificates at the time of session generation allows participants to send encrypted messages to each other. This possibility should be considered only for the transfer of information messages between hosts, but not as a system of event acknowledgments for a narrow number of verifiers. Thus, the possible ways of organizing the data storage format are shown in Fig. 4 summarized:

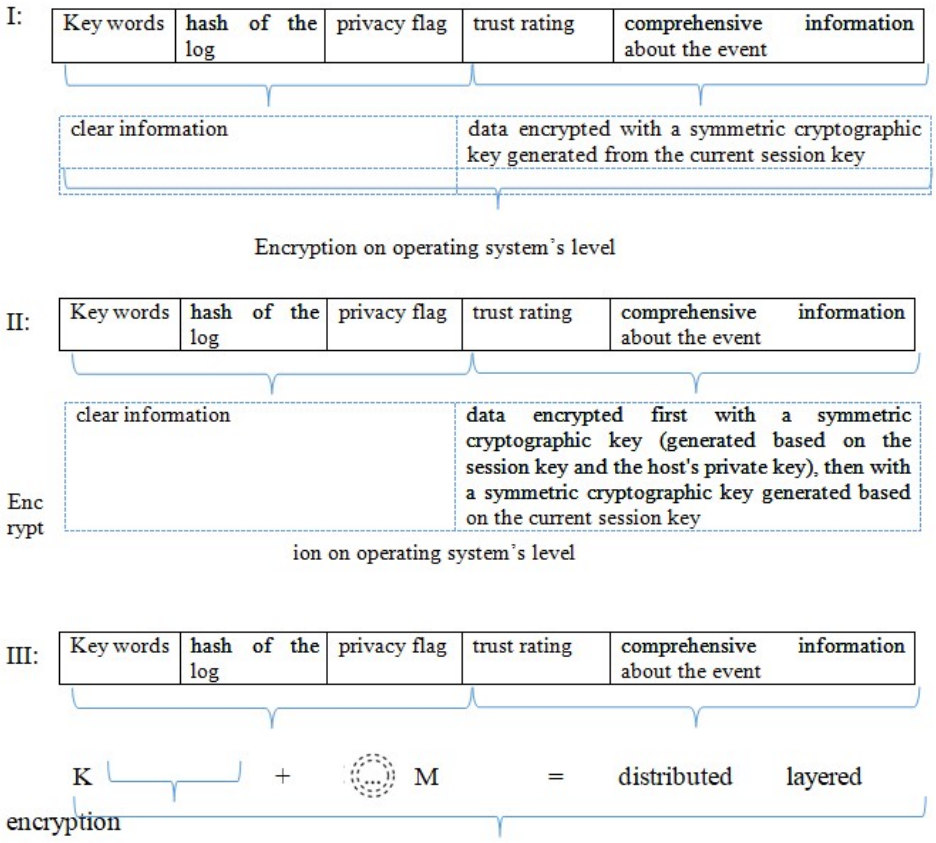


Fig. 4. An example of data to be written to the blockchain storage.

Method 1 was chosen as the main format to speed up data analysis by performing search queries on open records (key words) with subsequent decryption of the necessary information about events.

Format II implies the storage of private records for which network participants assign no trust rating. This involves multilayer encryption of confidential information.

There are many similar formats; they are optionally configured through the administration panel. In this case, various combinations of distributed multilayer encryption are possible, depending on the target needs and architecture of the computer network of the customer's enterprise. As an example, the format N is illustrated, where M is the number of encryption layers, and K is the number of field combinations for multilayer encryption M.

The latter is the most sophisticated approach to data storage, in which any combination of encrypted fields and any number of encryption layers are possible. The balance between the speed of the system and the level of security of information resources depends on the needs of the end consumer of the product.

It should be noted that, regardless of the selected data storage format, encryption is additionally carried out at the operating system level.

7. RELIABILITY And FAULT TOLERANCE ISSUES

Data protection in the normal mode of operation of the System is carried out by a symmetric cryptographic key generated based on the session key. If an attacker steals the database, he will not be able to decrypt it, since the last session key is not explicitly stored anywhere. Moreover, past session keys are encrypted for each host with asymmetric encryption.

The system administrator protects distributed Denial of Service (DDoS) attacks. A corporate computer network necessarily uses the intelligent functions of the managed network equipment; it cannot have resources for a DDoS attack. The system monitors and blocks nodes with suspicious network activity.

In the case of a tail-end attack, in which the attacker removes the first blocks of the chain (truncates the tail), the verifying host, if it does not know the original length of the hash chain, is unable to detect the fact of the attack. The solution to this issue is end-to-end numbering of all blocks, while the first block of the chain, the so-called genesis block, is assigned a number equal to zero.

The organization of network interaction in decentralized networks does not exclude the occurrence of collisions during the simultaneous processing of information flows. Two or more hosts could simultaneously identify a network event and broadcast it to the System for verification before writing to the blockchain storage. This entails two undesirable consequences: an increase in the volume of storage and a slowdown in the search for information on it. The second point is more critical: multiple recording of one event consumes the computing power of the network infrastructure. Such an event is offered to all clients of the system for checking many times before being written to the storage. Consequently, the participants in the network interaction, when checking this data, will spend resources to repeatedly generate confidence coefficients for information that is in fact the same event. Considering the possible rather large number of clients and their low processing power, such situations can greatly reduce the speed of writing to the storage.

To prevent the described situations on each client in the module of the distributed system for collecting, processing and analyzing events (element under number 2 in Fig. 1), it is proposed to perform preliminary processing (marking) of the local history of incidents, consisting of the following stages:

1) when an incident is detected, the identification coroutine places information about the event in the local storage of incidents, marking it as required to be stored in the blockchain;

2) the synchronization coroutine reads the latest incidents from the local storage and initializes saving them in the blockchain, if they are marked with the corresponding flag, and then marks them as saved. By default, they are not removed from the local storage, but can be optionally configured, including specifying the required time intervals for cleaning.

Full integration with a distributed system for collecting, processing and analyzing events not only avoids collisions, but also increases the speed of the System as a whole. When the client is offered the next event to check, he first searches his local storage. If he manages to find confirmation of the event, he immediately exposes him to the appropriate criterion of trust, without resorting to checking the incident by means of subroutines. If an event detected in the local storage is marked as requiring saving in the blockchain, the status "Saved by another client" is set to it. Thus, the synchronization coroutine in the client of the system will not send information about this incident to the blockchain, which prevents duplicate records in the main storage. If the client, while checking the next event, finds a retraction of the event by another incident, then he sets the corresponding coefficient for him. This does not change the status of an incident in the local storage, and the synchronization coroutine will be able to send information about this to the global storage at the next cycle. In this case, two records will be made in the system: the first one about incident A with a negative coefficient of confidence, and a record about incident Б with a positive coefficient of confidence. So record Б can be considered as refuting record A.

If the client, when checking an event, cannot find any records that confirm or deny the event being checked, he starts checking the event at the level of subroutines that use the means of operating systems, services and various programs. In this case, the process of generating the confidence factor will take more time due to the need to collect process and analyze data. This information is not recorded in the local storage, since the incident detection coroutine did not consider it necessary to consider it. The Client of the System just attempted to verify the incident. If the incident checking routines can neither confirm nor deny the event, then an appropriate confidence factor equal to zero is set to it.

It is possible to configure interaction with duplicate checks not only with a distributed system for collecting, processing and analyzing events, but also with agents of primary information collection. The balance between the redundancy of information, the consumed computing power and the speed of the method determines the profitability of the System configuration, depending on the tasks set. In general, the event processing procedure can be graphically depicted as follows (Fig. 5).

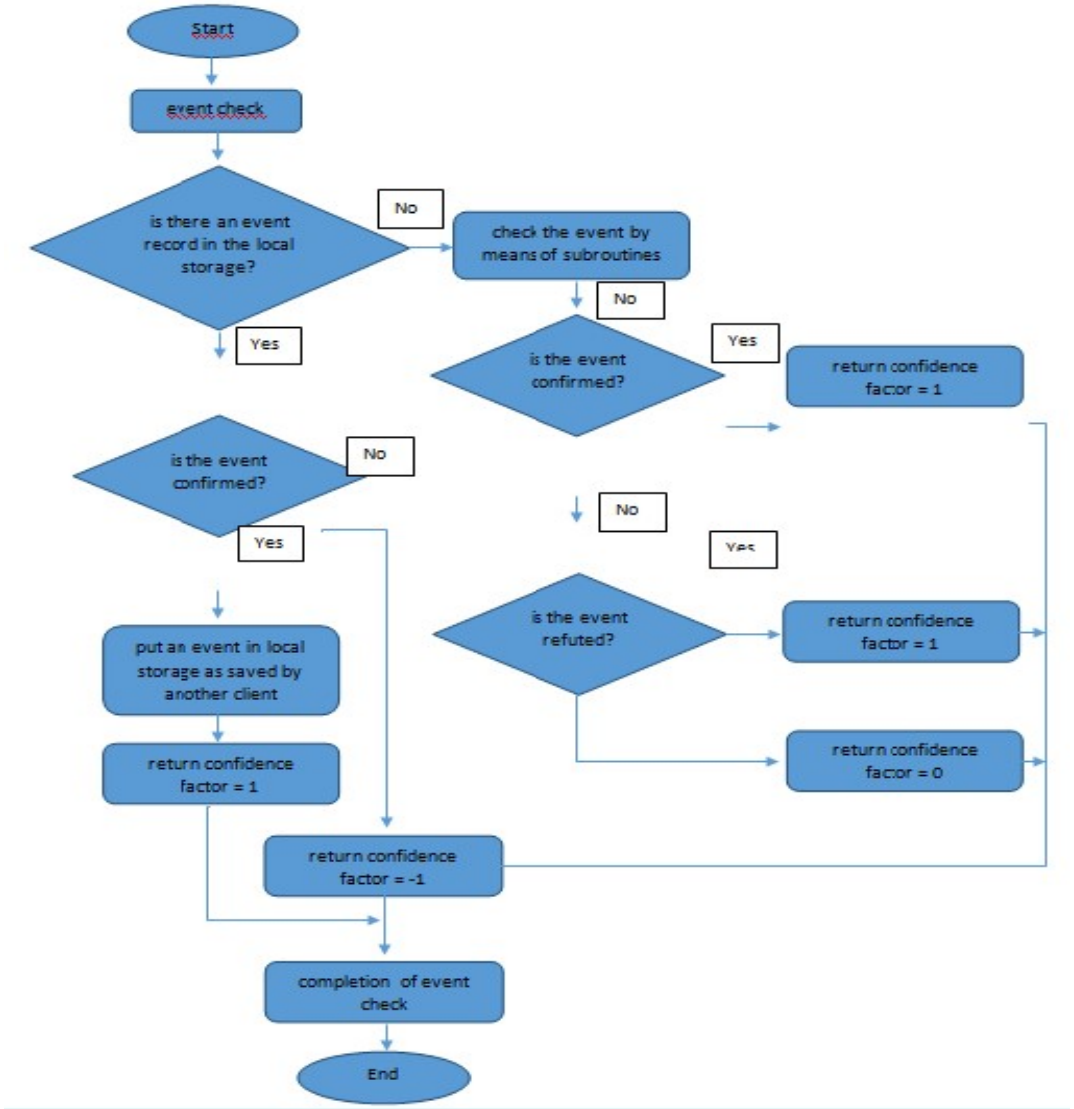


Fig. 5. Block Diagram Of The Event Handling Procedure

It is important to note that integration with a distributed system for collecting, processing and analyzing events can be configured in several ways, depending on the requirements of the technical assignment. In the first case, it will duplicate the information of the decentralized event register, adding redundancy, but increasing the speed of data access. In the second case, the local event storage will not include the information of the main blockchain. The entries in it will be of value only for a short or medium-term period of time, after which they will be deleted. The local storage after starting and before terminating the work of the System client will be cleared of obsolete records, thereby saving space on the hard disk. The third mode allows you to profile and distribute information over two sources, optimizing the speed of programs with different purposes. The choice of the integration method depends on the requirements of the technical specifications, including computing power and the amount of information in the enterprise's network infrastructure.

To assess the effectiveness of the proposed solution and confirm the operability of the hypotheses put forward, a technological con-veyer for the development of software products based on the DevSecOps methodology was built. Manual and automated testing was performed at each stage. For the purposes of experimental research, the software product (functioning on the basis of the method of system analysis, management and information processing of a corporate computer network) was

integrated into a real distributed multi-profile enterprise infrastructure with a number of 700 hosts. The corporate network was distributed and corresponded to the initial conditions and restrictions presented in the first section (TCP/IP protocol stack v4 and v6, Windows/ Linux/ Mac OS family OS, etc.).

As part of the first experiment, more than 10,000 iterations of network attacks and unauthorized impacts on various segments of the network were carried out using active traffic analysis tools and information resources, including scanners, probes and pentest tools. A wide range of tools were used: from the standard Kali Linux suite to proprietary products written on the basis of the Researcher framework. The situation illustrated in Figure 2 was reproduced, but in different network segments with different topologies and structures. As part of the experiment, the correctness of event processing was determined from the moment of identification to the assessment of trust in it, saving to the blockchain and organizing control actions. The experiment was binary, each stage of the method was processed correctly, each node provided a correct assessment of the confidence of the recorded information in each of the 10,000 iterations. Due to the specifics of the method, there is no need to talk about errors of the first and second kind, because the work does not affect the operation of the database and knowledge base of intrusion detection and prevention systems. For more than two years of continuous operation, the method has proven to be a reliable, fault-tolerant and secure solution. The size of the database of the distributed system for collecting, processing and analyzing events of the enterprise's network infrastructure ranged from 1.25 to 14.3% of the total volume of full-time knowledge bases of agents of primary information collection of various systems and services. The size of records of one host in the decentralized storage, taking into account multi-layer encryption, was 4 - 41.7% of the total volume of knowledge bases of local aggregators. Even with the duplication of all the listed knowledge bases, the introduction of redundancy is a low cost of improving the reliability, security and efficiency of the functioning of the enterprise's network infrastructure.

8. CONCLUSION

Within the framework of this article, an original method of system analysis, management and processing of information of a corporate computer network operating based on the TCP / IP protocol stack was presented. The scientific novelty of the proposed solution lies in the ability to automatically control the traffic of a computer network and local information processes of its hosts based on an objective and informative register of events, protected from various external disturbances (from impersonation attacks to falsification of records) by using a modified de-centralized blockchain storage with a trust management system for registered events. Another important aspect of scientific novelty is the profiling of access to information and protection of the data transmission process based on group and iterative multilayer encryption.

The contribution of the presented scientific and practical research to the general body of knowledge lies in the scientific novelty and practical significance of the proposed method, namely, in the possibility of effective and objective management of information flows and enterprise processes based on a reliable and independent event registration platform.

The software implementation of the method can be used as an additional module at the heart of intrusion detection and prevention systems, event collection, analysis and correlation systems. The proposed project can be used together with existing solutions [1-6], increasing their efficiency in real infrastructures where technologies of virtual secure communication channels and encryption protocols are used.

In the next issue of the journal, a method for the formation of a decentralized register of events of the information infrastructure of an enterprise, functioning based on the proposed approach, will be presented. It is planned to highlight the stage of design and software implementation of the solution, followed by an experimental study of the effectiveness of its operation.

REFRENCES:

[1] Bondjakov A.S. Osnovnye rezhimy raboty sistemy predotvrashhenija vtorzhenij (IDS/IPS SURICATA) dlja vychislitel'nogo klastera [Main modes of operation of the intrusion prevention system (IDS / IPS SURICATA) for the computing cluster] // Modern information technology and IT education. 2017. T. 13. № 3. S. 31–37. (in Russian)

[2] Efimov A.Ju. Problemy obrabotki statistiki setevogo trafika dlja obnaruzhenija vtorzhenij v sushhestvujushhih informacionnyh sistemah

[Problems of processing network traffic statistics for intrusion detection in existing information systems] // Software Products and Systems. 2016. № 1. S. 17–21. (in Russian)

[3] Docenko S.M. Sistemy obnaruzhenija vtorzhenij na osnove vstraivaemyh mikroprocessornyh sistem [Intrusion detection systems based on embedded microprocessor systems] / S.M. Docenko, A.G. Vladyko, I.D. Letenko // Telecommunications. 2013. № S7. S. 15–18. (in Russian)

[4] Chandre P.R. Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification / P.R. Chandre, P.N. Mahalle, G.R. Shinde // Proceedings of the IEEE Global Conference on Wireless Computing and Networking (GCWCN). - Lonavala, India. – 2018. - P. 135 – 140.

[5] Zitta T. Penetration Testing of Intrusion Detection and Prevention System in Low-Performance Embedded IoT Device / T. Zitta, M. Neruda, L. Vojtech, M. Matejkova and oth. // Proceedings of the 18th International Conference on Mechatronics - Mechatronika (ME). - Brno, Czech Republic. – 2018. – P. 1 – 5.

[6] Safonov M. Centralizovannoe hranenie zhurnalov [Centralized log storage] / Safonov M. // System Administrator. 2012. №. 5 (114). S. 28–33. (in Russian)

[7] Basinya E. A. Raspredelennaja sistema sbora, obrabotki i analiza sobytij informacionnoj bezopasnosti setevoj infrastruktury predprijatija [Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure] / IT Security. 2018. T. 25. № 4. S. 43–52. (in Russian)

[8] Francuzova, G. A. Samoorganizujushhajasja sistema upravlenija trafikom vychislitel'noj seti: metod protivodejstvija setevym ugrozam [Self-organizing computer network traffic management system: a method to counteract network threats] / G.A. Francuzova, A.V. Gun'ko, E.A. Basinya // Software engineering. – 2014. – № 3. – S. 16–20. (in Russian)

[9] Basynya EA The system of intelligent-adaptive management of the information infrastructure of the enterprise / EA Basynya // Information technologies = Informatsionnye tekhnologii: scientific and technical. zhurn. - 2020. - No. 5 (26). - S. 283–289. - DOI: 10.17587 / it.26.283-289. - The work was carried out: with the support of the Russian Foundation for Basic Research (No. 18-00-00238).

[10] Basinya E. A. Automatic traffic control system for SOHO computer networks / E. A. Basinya, A. A. Rudkovskiy // Studies in Systems, Decision and Control. - 2019. - Vol. 119 : Recent Research in Control Engineering and Decision Making. ICIT 2019. - P. 743-754. - DOI: 10.1007/978-3-030-12072-6_60.

[11] Basinya E. A. Countermeasure method against unauthorized and anonymous information system data collection [Electronic resource] / E. A. Basinya, V. E. Khitsenko, A. A. Rudkovskiy // Dynamics of systems, mechanisms and machines (DYNAMICS) : proc., 13 intern. sci. and techn. conf., Omsk, 5–7 Nov. 2019. – IEEE, 2019. – 6 p. - Mode of access: https://ieeexplore.ieee.org/document/8944715/authors#authors. - Title from screen - ISBN 978-1-7281-0970-1. - DOI: 10.1109/Dynamics47113.2019.8944715.B

[12] Basinya E. A. Development of a comprehensive security system [Electronic resource] / E. A. Basinya, A. A. Yushmanov // Dynamics of systems, mechanisms and machines (DYNAMICS) : proc., 13 intern. sci. and techn. conf., Omsk, 5–7 Nov. 2019. – IEEE, 2019. – 7 p. - Mode of access: https://ieeexplore.ieee.org/document/8944700/authors#authors. - Title from screen - DOI: 10.1109/Dynamics47113.2019.8944700.

[13] Basynya E. A. Method for forming a decentralized registry of the enterprise information infrastructure events / E. A. Basynya, A. V. Safronov // Bulletin of the Ural Federal District. Information security = Journal of the Ural Federal District Information security. - 2019. - No. 4 (34). - S. 35-44.

[14] Basynya E.A. Method to identify cybercriminals using network analysis of information systems with anonymization / E. A. Basynya, V. E. Khitsenko, A. A. Rudkovsky // Reports of the Tomsk State University of Control Systems and Radioelectronics. - 2019. - T. 22, No. 2. - P. 45–51. - DOI: 10.21293 / 1818-0442-2019-22-2-45-51.