IRSTI 81.93.29 https://doi.org/10.26577/JMMCS-2019-3-m6

Analysis of intrusion detection systems

Zhumangaliyeva N.K., K.I. Satpayev Kazakh National Research Technical University,
Almaty, Kazakhstan, E-mail: nazym_k.81@mail.ru
Korchenko A.A., National Aviation University, Kyiv, Ukraine,
E-mail: annakor@ukr.net
Doszhanova A.A., Almaty University of Power Engineering and Telecommunications,
Almaty, Kazakhstan, E-mail: d_alia.81@mail.ru
Avkurova Zh. S., L.N.Gumilyov Eurasian National University,
Nur-Sultan, Kazakhstan, E-mail: zhadyra.avkurova.83@mail.ru

With the development of information technologies, the amount of vulnerabilities and threats to various data processing systems is increasing, therefore specialized means of security are required to ensure their normal operation and to prevent intrusions, and a promising area that is actively developing in the field of information security is the detection of cyber attacks and the prevention of intrusions in information systems from the unauthorized side. In order to detect network intrusions there are used modern methods, models, tools and complex technical solutions for intrusion detection and prevention systems, which can remain effective when new or modified types of cyber threats appear. Therefore, there was conducted a generalized analysis of the intrusion detection systems software based on a certain basic set of characteristics («Cyber Attack Class», «Adaptability», «Detection Methods», «System Control», «Scalability», «Observation Level», «Reaction to Cyber Attack», «Security» and «Operating System Support»). It will give certain opportunities for choosing such tools and for developing the most effective security mechanisms during cyber attacks.

Key words: attacks, cyber attacks, anomalies, anomaly detection in information systems.

Басып кіруді анықтау жүйелерін талдау

Жумангалиева Н.К., Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті,
Ақпарттық және телекоммуникациялық технологиялар институты,
Алматы қ., Қазақстан, E-mail: nazym_k.81@mail.ru
Корченко А.А., Ұлттық авиациалық университет,
Киев қ., Украина, E-mail: annakor@ukr.net
Досжанова А.А., Алматы энергетика және байланыс университеті,
Алматы қ., Қазақстан, E-mail: d_alia.81@mail.ru
Авкурова Ж.С., Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Нұр-Сұлтан қ., Қазақстан, E-mail: zhadyra.avkurova.83@mail.ru

Ақпараттық технологиялардың дамуымен мәліметтерді өңдеудің әртүрлі жүйелеріне осалдықтар мен қауіп-қатерлер саны ұлғаюда, сондықтан олардың қалыпты жұмыс істеуін қамтамасыз ету және басып кіруді болдырмау үшін арнайы қауіпсіздік құралдары қажет, ал ақпараттық қауіпсіздік саласында белсенді дамып келе жатқан бағыт кибершабуылдарды анықтау және авторланбаған тарап тарапынан ақпараттық жүйелерде басып кіруді болдырмау болып табылады. Желілік басып кіруді анықтау үшін киберқауіптердің жаңа немесе модификацияланған түрлері пайда болған кезде тиімді болып қалуы мүмкін басып кіруді анықтау және болдырмау жүйелері үшін қазіргі заманғы әдістер, модельдер, құралдар және кешенді техникалық шешімдер қолданылады. Сондықтан, жұмыста белгілі бір базалық сипаттамалар бойынша («кибершабуылдар класы», «бейімделу», «анықтау әдістері», «жүйені басқару», «масштабтал», «бақылау деңгейі», «кибершабуылға әсері», «қорғалу» және «операциялық жүйені қолдау») басып кіруді анықтау жүйесінің бағдарламалық құралдарына жалпылама талдау жүргізілді. Кибершабуылдардың әсер етуі кезінде осындай құралдарды таңдау және олар үшін қауіпсіздіктің ең тиімді тетіктерін әзірлеу бойынша белгілі бір мүмкіндіктері болып табылады.

Түйін сөздер: шабуылдар, кибершабуылдар, ауытқулар, ақпараттық жүйелерде ауытқуды анықтау.

Анализ систем обнаружения вторжений

Жумангалиева Н.К., Казахский национальный научно-исследовательский технический университет имени К.И.Сатпаева, Институт информационных и телекоммуникационных технологии, г. Алматы, Казахстан, E-mail: nazym_k.81@mail.ru
Корченко А.А., Национальный авиационный университет, г. Киев, Украина, E-mail: annakor@ukr.net
Досжанова А.А., Алматинский университет энергетики и связи, г. Алматы, Казахстан, E-mail: d_alia.81@mail.
Авкурова Ж.С., Евразийский национальный университет имени Л.Н. Гумилева, г. Нур-Султан, Казахстан, E-mail: zhadyra.avkurova.83@mail.ru

С развитием информационных технологий увеличивается количество уязвимостей и угроз различным системам обработки данных, поэтому для обеспечения их нормального функционирования и предотвращения вторжений необходимы специализированные средства безопасности, а перспективным направлением, которое активно развивается в сфере информационной безопасности является выявление кибератак и предотвращения вторжений в информационных системах со стороны неавторизованной стороны. Для обнаружения сетевых вторжений используются современные методы, модели, средства и комплексные технические решения для систем обнаружения и предотвращения вторжений, которые могут оставаться эффективными при появлении новых или модифицированных видов киберугроз. .Поэтому, в работе проведен обобщенный анализ программных средств систем обнаружения вторжений по определенной базовой множеством характеристик («Класс кибератак», «Адаптивность», «Методы выявления», «Управление системой», «Масштабируемость», «Уровень наблюдения», «Реакция на кибератаку», «Защищенность» и «Поддержка операционной системы»). Это даст определенные возможности по выбору таких средств и разработки для них наиболее эффективных механизмов безопасности при воздействиях кибератак.

Ключевые слова: атаки, кибератаки, аномалии, обнаружения аномалий в информационных системах.

1 Introduction

The rapid development of information systems (IS) and technologies comprehensively affects all areas of society. A significant amount of modern public and private enterprises use IS to control production processes, for decision-making support, for necessary data search. At the same time, the amount of vulnerabilities and threats to IS is increasing, and therefore, in order to ensure their normal operation and to prevent intrusions threre are needed specialized security tools. It should be noted that one of the current areas that is actively developing in the field of information security is cyber attacks detection and intrusions prevention in IS from the unauthorized side. For example, a number of recently implemented cyber attacks, which caused damage to many public institutions and private enterprises and organizations showed the unavailability and imperfection of their own security systems at previously unknown intrusions. Mass cyber attacks initiate the creation of special technical solutions, means and systems of counteraction. In order to detect network intrusions, there are used modern methods [4–12], models [12], tools [12, 14–16], software [12, 17–27] and complex technical solutions for intrusion detection and prevention systems [8, 12, 15, 22, 27-29], which can remain effective when new or modified types of cyber threats occur. But in practice, with the occurrence of new threats and anomalies generated by attacking actions with unspecified or unclearly defined properties, these means do not always remain effective and require long time resources for their adaptation. Therefore, intrusion detection systems (IDS) must be constantly researched and improved to ensure continuity in their effective operation. Among such systems are specialized software tools that are aimed at identifying suspicious activity or interference in IS and for taking adequate measures to prevent cyber attacks. These systems and tools, as a rule, are quite expensive, have a closed code and require periodic support from developers (highly qualified specialists) for their improvement and appropriate adjustment to the conditions of specific organizations. On this basis, the analysis of technical solutions, special tools and software for the detection of cyber attacks, misapplication and anomalies in the IS for their use in selecting and developing IDS, as well as determining the most effective appropriate protection mechanisms for OS is an urgent task. Shadow and SnortNet software is described in [10, 20, 24, 26, 30], which is used in order to detect violations of such characteristics as "Cyber Attack Class", "Adaptability", "Detection Methods", "System Control", "Scalability", "Observation Level", "Reaction to Cyber Attack", "Security"and "Operating System (OS) Support". But for a more objective assessment of modern software, it is important to consider a much wider range of relevant implementations, for example, Cisco IPS, Kaspersky Anti-Targeted Attack Platform, InfoWatch ASAP, Tipping Poing NGIPS, Arbor Networks Spectrum and etc. In addition, [7, 8, 12, 15, 17, 21-23, 25, 26] provides a general description of the individual functions and operating principles of EMERALD, OSSIM, CMDS, Shadow, Network Flight Recorder, Tripwire, NetProwler, NetRanger, Centrax and RealSecure, but no analysis was conducted regarding the basic characteristics of "Detection Methods", "Reaction to Cyber Attacks", "Security"and etc.

Also in [27] there are revealed the basic principles for the operation of the most popular IDS of 2018 – SolarWinds Log and Event Manager, Suricata, Sagan, Security Onion, AIDE, OpenWIPS-NG and Fail2Ban — and the operating systems with which they are supported are defined, but no analysis has been made regarding basic characteristics "Cyber Attack Class", "Adaptability", "Security" and etc. In [18] there are compared the functionality of RealSecure, NetProwler and Outpost, but this work does not describe the generalized approaches and does not analyze the modern tools of Symantec DeepSight Threat Management System, Arbor Networks Spectrum, AxoftinvGUARD, DefensePro, etc., there are do not defined the features regarding the basic characteristics "Reaction to Cyber Attacks", "Cyber Attack Class", "Adaptability", "Detection Methods" and etc.

Works [6, 7, 15] described a number of methods used in software for detecting attacks and anomalies, but no assessment was made regarding the characteristics "Scalability", "Observation Level" and "Reaction to Cyber Attacks".

Also in [1] there are considered intrusion detection and prevention systems, the operation of which is based on network traffic anomalies (anomalous intrusion detection and prevention systems), in [12, 15] there are described methods and models used for intrusion detection, in [4-6 , 8, 9, 11, 29] there are compared methods of attacks and anomalies detection, and the work [29] focuses on the use of fuzzy logic for the effective detection of anomalies. But no one of the sources did not carry out a study of specific software, assessment of its properties and description of basic characteristics.

2 Literature review

Anomalies are patterns in data that do not conform to the expected normal behavior An anomaly detection system (ADS) constructs a profile of expected normal behaviourusing data , collectedov eraperiodofnormal(attack-free)operation. Modern methods for anomaly detection in intrusion detection systems O. M. Kolodzik Computer systems and networks. 2012. Cases of complex attacks on IS are becoming more frequent[1-3]. In there was proposed a classification of IDS and intrusion prevention systems, their advantages and disadvantages and some features of construction were indicated, and in there was carried out a classification to identify network intrusions (anomalies and intruders), but existing software is not considered with respect to certain basic characteristics. [7] In the works there are considered the main features, principles of construction, functioning mechanisms and comparative analysis of IDS, but there is no specific research of software about the characteristics of "Cyber Attack Class", "Adaptability", "Detection Methods" and etc. Zhumangaliyeva N. developed Rating for attack detection system II international scientific and practical conference proceedings 2016. Analysis of the examination method In there was conducted an analysis regarding the construction of attack detection systems, there In another paper, the authors [3] V. V. Litvinov are shown the basic principles of creating countermeasures against cyberattacks, but there is no analysis regarding the specific software about the characteristics "Scalability", "Observation Level", "Reaction to Cyber Attacks" and etc. [10] R. Patel, A. Thakkar, A. Ganatra. There are many publications and research projects on the application of cybersecurity analysis For example, the authors Marcus Ranum, Network Flight Recorder, The ability to protect or defend the use of cyberspace from cyber-attacks and used the term as one word. In 2014 [2] An analysis of the sources showed that for modern IS and networks there is an acute issue of prompt detection of misapplications and anomalies. In the majority of these works, only a partial analysis of IDS and their classification is given, a general description of the corresponding software is presented, which does not reflect their broad spectrum and does not contain the necessary set of characteristics for the integrated assessment of such systems. [14] Based on this, the aim of the work is to conduct a generalized analysis of the IDS software on a certain basic set of characteristics. This will provide certain opportunities for the selection of such tools and the development of the most effective security mechanisms for them under cyber attacks. As a rule, methods for attacks detection are divided into methods for misapplications and anomalies detection the authors B. Eriksson, R. Durairajan, and P. Barford. Riskroute: a framework for mitigating network outage threats. InCoNEXT, 2013. Misapplications are based on the use of existing IS disadvantages. The main difference between an anomaly and misapplication is that an anomaly is a process that occurs before a possible intrusion into the system or indicates the presence of an already existing attack classification of intrusion detection systems A.A. Korchenko, B.S. Akhmetov [15]. In fact, the anomaly is a deviation from the normal state of the system, an unusual activity in it, which may indicate certain attacking actions. It should be noted that the anomaly may occur by other reasons, for example, due to improper operation of the system. Kaspersky Anti Targeted Attack Platform [Electronic resource] // Kaspersky Lab. M. : JSC Kaspersky Lab, 2016. P. 1-12. [23]

3 Material and methods

That is why with the help of an effective analysis of anomalies arising in the system, it is possible to prevent certain types of cyber attacks and take the necessary measures to block them and to protect IS in time. It should be noted that the widespread use of modern means of protection against cyber attacks does not guarantee security at the proper level, since recently:

- attacks directed at corporate systems, public, confidential and government information resources are growing;
- cyber attacks are constantly being modified, improved and become more regular;
- detection of cyber attacks by classic remedies is not always effective;
- cases of complex attacks [1-3] on IS are becoming more frequent.

It is also associated with the intensive development of software and hardware and the globalization of information networks and their daily use in all areas of society.

Taking into account the results of well-known researches, followed by their generalization and reflecting on an extended range of tools for misapplication and anomalies detection, we will analyze the modern IDS with respect to the basic characteristics of the "Cyber Attack Class", "Adaptability", "Detection Methods", "System Control", "Scalability", "Observation Level", "Reaction to Cyber Attacks", "Security" and "OS Support" (see Table 1).

Before starting the analysis, we will reveal each of these basic characteristics.

"Cyber Attack Class" – defines the ability of the system to detect anomalies and misapplication at different levels of IS. Most modern tools have the ability to identify both classes of attacks (anomalies and misapplication) [3].

"Adaptability" allows the system effectively to adapt to new attacks (missing in the signature database), for example, 0-day and to detect cyber attacks with minor modifications [30].

"Detection methods" are the sets of methods used to detect attacks and to form the mathematical basis of the system. The most common are the methods of statistical and cluster analysis, events changes control, attack graphs signature, dynamic, machine learning, behavioral, heuristic, expert, fuzzy sets, etc. [15].

"System Control" – defines the control scheme and its level. Control can be carried out centrally from a single host or distributed from individual hosts connected by one system. The most optimal is the organization of control under a centralized scheme with some set of centers, each of which can be used to control the entire structure [30]. Centralized systems implement the control of all means (modules) of detection of anomalies and misapplications from one station and distributed ones implements the control separately, where each module is responsible for its function.

"Scalability" is the ability to expand the system, its adaptability to various network structures and the addition of new analyzed network resources [30].

"Observation Level" – determines at which level of the system data is obtained for cyber attacks detection. Two levels of data acquisition are applied - network and system. Modern systems, as a rule, support both levels of observation, since their interaction provides better protection. The speed of the formation of primary data, their correct processing and obtaining accurate information about the current state of the OS [30] depends on this characteristic.

Network traffic analysis is performed using special sensors (network and system), which are used in the attacks and anomalies detection systems. Network sensors analyze data at the network level (usually based on signature analysis) and generate a cyber attack detection message and send it to the control modules.

System sensors analyze the OS logs, applications and software applications for possible anomalies or threats and generate corresponding messages to control modules [30].

"Reaction to cyber attack" – determines the presence in the system of components or modules of counteraction. That is, after registration of the attack, actions are initiated to reduce further negative impact [30].

"Security" – describes the presence of its own components of the system, which are responsible for protecting it from cyber attacks and external negative information impact, as well as for the resistance to failure and for reducing the amount of development vulnerabilities in general [30].

"OS support" – describes the type of OS (for example, Unix, Linux, Windows, MacOS, etc.) that supports the corresponding system software.

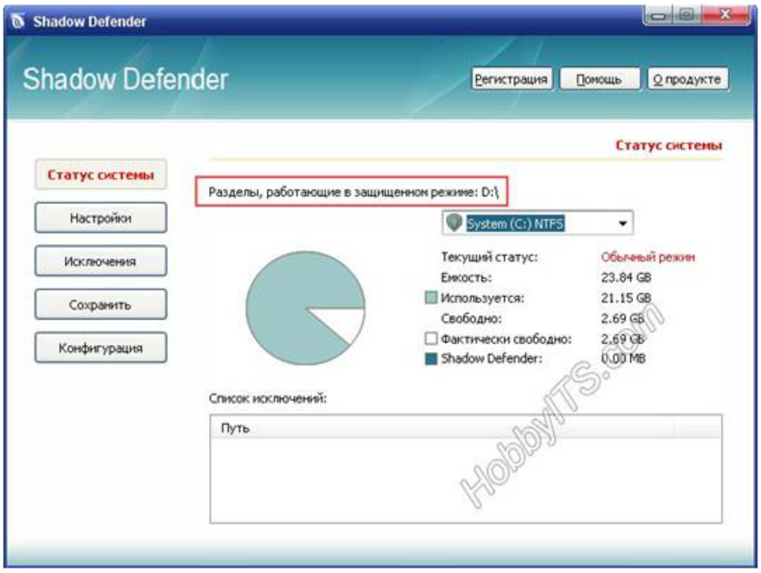
Further, taking into account the proposed characteristics, we will reveal the properties of the corresponding IDS (see Table 1).

3.1 Software is able to detect attacks and anomalies.

The Network IDS Shadow (Secondary Heuristic Analysis for Online Defensive Warfare, manufacturer is Naval Surface Warfare Center (Naval Center), Virginia, USA) contains sensor stations and analyzer stations. The first ones are located on the outside of the firewalls, and the second ones – in the internal secure network segment. A sensor station is a server on which tcpdump is activated, which writes traffic to a file. Sensors select package headers and store them in a special file. The analyzer station reads this information, filters it and generates the corresponding log. If events are identified and there is a response strategy for them, then alert messages are not generated. Sensors are used to extract packages of the libpcap utility, and the main analysis takes place in the tcpdump module, which contains packet filters, divided into simple and complex (from several filters). In fact, the system uses a number of Perl language filters, sensors and analyzers. Shadow (Fig. 1) also functions on many UNIX systems, including FreeBSD and Linux, and uses the web interface to display information . Due to the flexibility of the Perl language, the architecture used in Shadow is one of the best networked IDSs.

The system is focused on identifying misapplications and simple anomalies using the network state monitoring method, which provides the system with the full possibility of adaptability to new cyber attacks. Shadow has a closed source code, and the corresponding extensions are carried out only by the developer. The sensor and sensor system allows to detect cyber attacks based on monitoring changes in network characteristics using the use of status logs and certain software filters. System control is distributed through configuration files on all nodes where system components are located. The Shadow architecture allows to create sensors (located in network nodes to collect information and to write to the log) and analyzers (analyze all events recorded to the log using sensors) to detect attacks at various network levels, regardless of its size [22].

The structural features of this system allow cyber attacks detection only at the network level [6]. For its security, Shadow uses the SSH protocol, but does not contain special anti-intrusion mechanisms and is not resistant to possible targeted cyber attacks. It is supported



Разделы, работающие в защищенном режиме: D:\

System (C:) NTFS

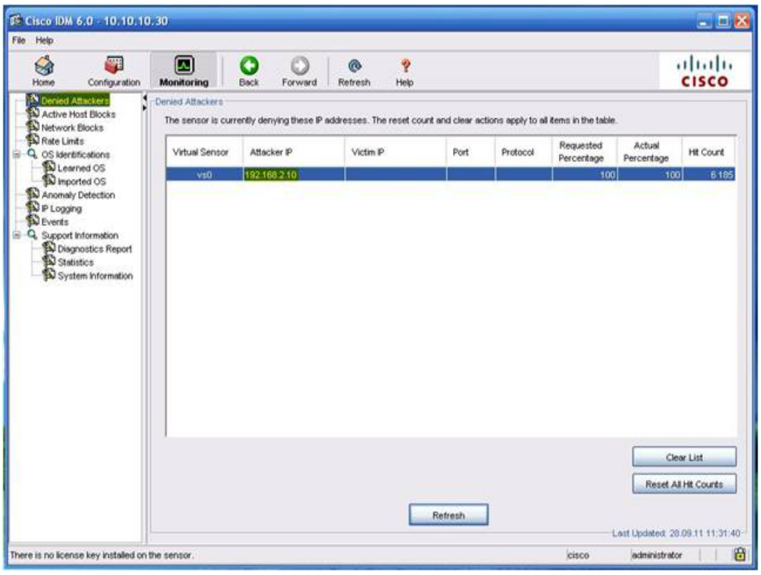
Текущий статус: Обычный режим
Емкость: 23.84 GB
□ Используется: 21.15 GB
Свободно: 2.69 GB
□ Фактически свободно: 2.69 GB
■ Shadow Defender: 0.00 MB

Список исключений:

Путь

Figure 1: Shadow working window

by the Kali Linux OS (Unix and Linux), it is part of the Snort software product and works in passive mode to collect data about the system. Cisco IPS



The sensor is currently denying these IP addresses. The reset count and clear actions apply to all items in the table.

Virtual Sensor	Attacker IP	Victim IP	Port	Protocol	Requested Percentage	Actual Percentage	Hit Count
vs0	192.168.2.10				100	100	6 185

Last Updated: 28.09.11 11:31:40

There is no license key installed on the sensor.

cisco administrator

Figure 2: Monitoring of IPS Sensors Using Cisco IPS

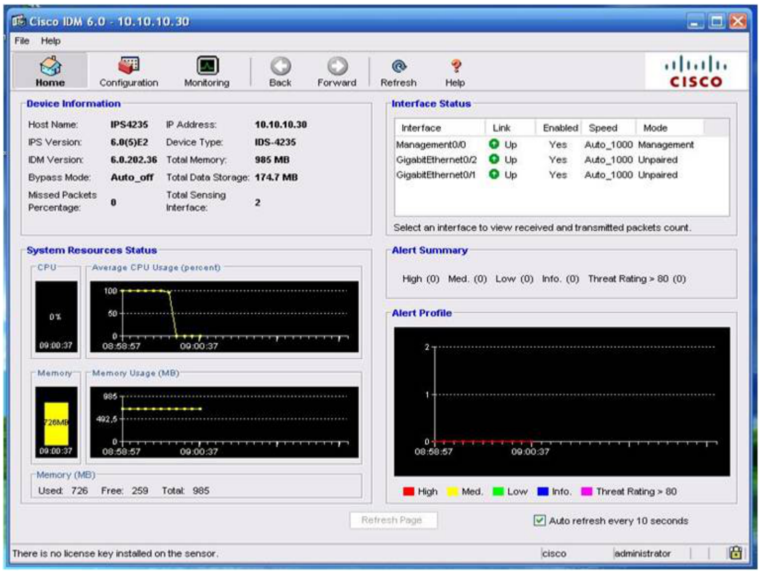
Cisco IPS implements deep packet surveillance function, which effectively counteracts a wide range of network cyber attacks. The control element is represented by the Cisco IOS integrated threat monitoring control system and is complemented by the Cisco IOS Flexible Packet Matching feature. This tool allows a computer network effectively to operate, taking into account the following factors:

- network availability control (provides network (distributed) protection against many attacks, exploits, worms and viruses);
- source cyber attack source detection rate and operational countermeasure implementation;
- deployment flexibility and scalability (interactive inspection of traffic using any combination of LAN interfaces and a WAN router configured on countraction to specific cyber attacks according to the risk level);
- working with the Cisco IOS firewall (monitoring of security features of Cisco IOS Software) [27].

Cisco IPS is a closed software and hardware complex with a large range of settings for network features and for the detection of intrusions using the available signature templates and certain statistical information. The system can be managed centrally or distributedly, depending on the complexity of network creation. Rapid, scalable system deployment is accomplished through dynamic policy control and the installation of the necessary components, taking into account the structure and characteristics of the network. Cisco IPS works only on FTP and HTTP / HTTPS servers using Unix, Linux and Windows OS [24].

Arbor Networks Spectrum.

Arbor Networks Spectrum (developed by Arbor Networks, Massachusetts, USA) is a high-performance solution for analyzing network traffic, determining damage from information security incidents, and detecting intrusions using a combination of statistical, dynamic and signature analysis methods. The main functionality of the Arbor Networks Spectrum (Fig. 3) [14] is the detection of DoS and DDoS attacks, trojans and their derivatives.



Host Name:	IPS4235	IP Address:	10.10.10.30
IPS Version:	6.0(5)E2	Device Type:	IDS-4235
IDM Version:	6.0.202.36	Total Memory:	985 MB
Bypass Mode:	Auto_off	Total Data Storage:	174.7 MB
Missed Packets Percentage:	0	Total Sensing Interface:	2

Interface	Link	Enabled	Speed	Mode
Management0/0	Up	Yes	Auto_1000	Management
GigabitEthernet0/2	Up	Yes	Auto_1000	Unpaired
GigabitEthernet0/1	Up	Yes	Auto_1000	Unpaired

Select an interface to view received and transmitted packets count.

High (0) Med. (0) Low (0) Info. (0) Threat Rating > 80 (0)

Memory (MB)
Used: 726 Free: 259 Total: 985

☑ Auto refresh every 10 seconds

There is no license key installed on the sensor. cisco administrator

Figure 3: View window of threat indicators in time

Arbor can be deployed as a device, a virtual solution for tracking network traffic, providing constant detection of cyber attacks and reducing their consequences. Arbor's patented Cloud Signaling technology successfully integrates this protection with cloud technologies, automating a key component of DDoS protection and reducing the time needed to reduce attacks. Hybrid multilayered protection is used. It is a fairly effective approach to protecting data from DDoS, which ensures the security of corporate networks no matter what type of DDoS attacks are directed against them. Arbor also has highly efficient control services that provide a high level of protection against counter-cyber attacks around the world. These services online in the global space have round-the-clock support from specialists for the reduction of DDoS attacks and for continuous intelligence in the field of threats [26].

3.2 Specialized software and hardware complex InfoWatch

The specialized software and hardware complex InfoWatch ASAP (InfoWatch Automation System Advanced Protector, developed by InfoWatch, Russia) is positioning itself as an intelligent solution for detecting and preventing cyber attacks aimed at the information infrastructure of automatic control systems for industrial and technological processes. Thanks to the proposed approach and patented protection technologies, the solution has several advantages over regular intrusion prevention tools that are implemented by manufacturers of modern equipment [27].

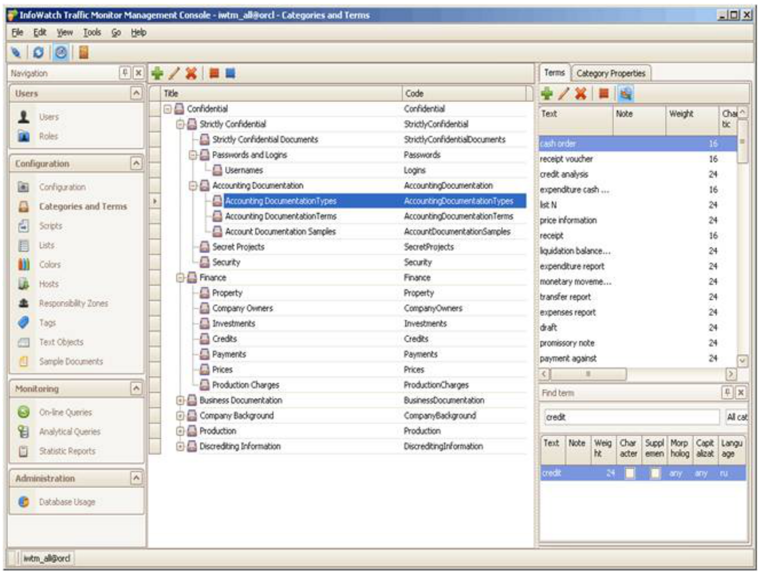
The InfoWatch ASAP complex (Figure 4) is designed to create security systems, is adapted for use in technological networks and is able to detect:

- targeted attacks at the level of automatic control and input or output of data by executive devices;
- intrusion (signature and statistical analysis) and anomalies in the characteristics of the technological IS;
- commands for changing settings and firmware of process equipment;
- unauthorized network connections;
- leakage of information about the state of the technological process;
- vulnerabilities in technological IS [25].

The main components of InfoWatch ASAP include modules:

- firewall;
- security monitoring and analysis;
- detection and prevention of intrusions;
- control of correct execution;
- technological process.

Also to InfoWatch ASAP include auxiliary components:



Title	Code
Confidential	Confidential
Strictly Confidential	StrictlyConfidential
Strictly Confidential Documents	StrictlyConfidentialDocuments
Passwords and Logins	Passwords
Usernames	Logins
Accounting Documentation	AccountingDocumentation
Accounting DocumentationTypes	AccountingDocumentationTypes
Accounting DocumentationTerms	AccountingDocumentationTerms
Account Documentation Samples	AccountDocumentationSamples
Secret Projects	SecretProjects
Security	Security
Finance	Finance
Property	Property
Company Owners	CompanyOwners
Investments	Investments
Credits	Credits
Payments	Payments
Prices	Prices
Production Charges	ProductionCharges
Business Documentation	BusinessDocumentation
Company Background	CompanyBackground
Production	Production
Discrediting Information	DiscreditingInformation

Text	Note	Weight	Cha tic
cash order		16	
receipt voucher		16	
credit analysis		24	
expenditure cash ...		16	
list N		24	
price information		24	
receipt		16	
liquidation balance...		24	
expenditure report		24	
monetary moveme...		24	
transfer report		24	
expenses report		24	
draft		24	
promissory note		24	
payment against		24	

credit

Text	Note	Weight	Character	Supplemen	Morpholog	Capitalizat	Language
credit		24	□	□	any	any	ru

Figure 4: InfoWatch Traffic Monitor report window

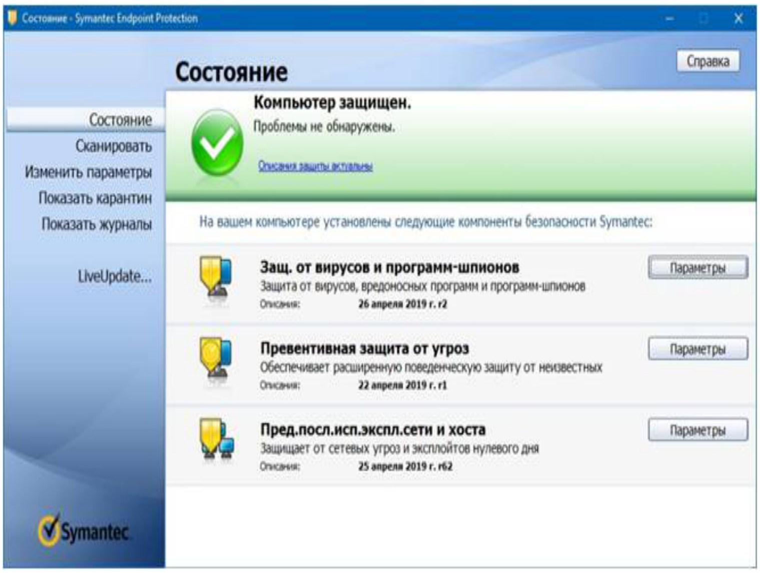
- network security module;
- analytics and data storage subsystem;
- graphical user interface.

The modular structure allows InfoWatch ASAP to function in monitoring, informing and warning modes and to detect cyber attacks and anomalies at different levels of the network (external and internal attacks on the information structure of the enterprise).

Symantec DeepSight. The Symantec DeepSight system (Symantec DeepSight Threat Management System, developed by Symantec, California, USA) allows to extend protection by providing early warning of active attacks, potential threats, new vulnerabilities, spyware, adware, which allows administrators more accurately to predict and to assess the degree of risk, as well as to prioritize information resources that require high-priority protection against intrusions. Also, the presence of sending personalized messages, which are complemented by professional threat analysis, generalized assessments and support for the choice of actions, make the Symantec DeepSight Threat Management System (Figure 5) the leading global cyber attack early warning system. The system has a fairly extensive infrastructure in global cyberspace, which consists of a number of honeypot networks.

With this system, you can analyze incoming data flows to computers through the network and to block threats before they are implemented in the system. Among the features of the work of this software there should be noted:

- automatic prioritization of existing threats and system resources, which allows quickly to establish the necessary level of resistance or protection;
- expert analysis of data that is collected from thousands of sources in global cyberspace, including information on active global attacks;



Состояние

Компьютер защищен.
Проблемы не обнаружены.
Описания защиты актуальны

На вашем компьютере установлены следующие компоненты безопасности Symantec:

Защ. от вирусов и программ-шпионов
Защита от вирусов, вредоносных программ и программ-шпионов
Описания: 26 апреля 2019 г. r2

Превентивная защита от угроз
Обеспечивает расширенную поведенческую защиту от неизвестных
Описания: 22 апреля 2019 г. r1

Пред.посл.исп.экспл.сети и хоста
Защищает от сетевых угроз и эксплойтов нулевого дня
Описания: 25 апреля 2019 г. r62

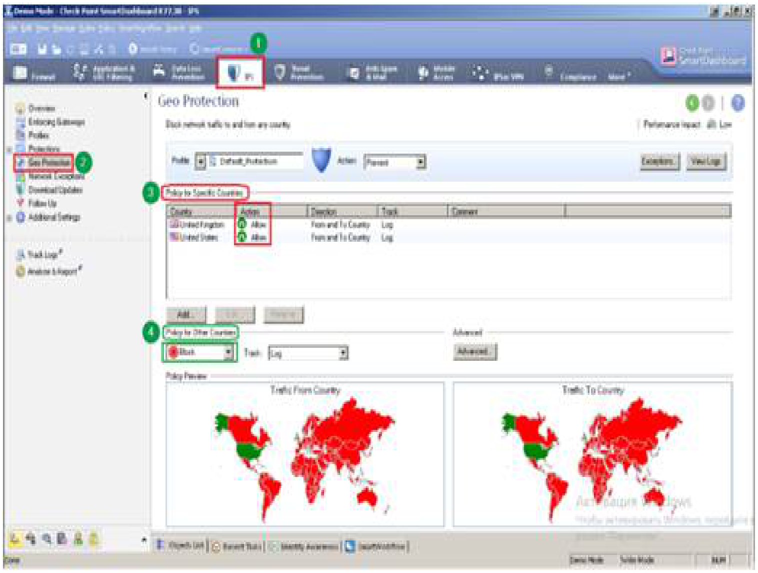
Figure 5: Symantec DeepSight Threat Management System window

- the constant increase and expansion of databases of existing network threats, through the wide distribution of this software product;
- automated monitoring of computer networks in real time, with the ability quickly to notify about the threat;
- analysis of existing and potential threats in the system and the creation of a basic strategy for their prevention;
- control of the software by special monitors of the functioning control, depending on the features of the system;
- a threat reduction strategy that allows the best prioritization, allocation and deployment of personnel and related security resources;
- accurate analysis that meets the requirements of a particular system, taking into account its network structure, organization features and activities [26].

This software is able to detect attacks and anomalies.

3.3 Intrusion Prevention System Software

IPS (Intrusion Prevention System Software Blade, developed by CheckPoint, USA), designed to prevent intrusions and is oriented on the complement of the security features of firewalls to protect against malicious and unwanted network traffic, including DoS and DDoS attacks, vulnerabilities in applications and servers (Application and server vulnerabilities), insider threats and etc. The Intrusion Protection System provides full and active intrusion prevention and consists of the IPS base product (Figure 6) and a number of Check Point Software add-on programs. With their help, it is quite easy to scale and to adapt the system to the needs of the network. Also, IPS allows automatic activation of network and system protection, even in the absence of administrative control. The system also provides comprehensive network protection (without degrading the gateway's performance) against unwanted traffic, IM and P2P, including detection and prevention of existing exploits, known and unknown vulnerabilities, tunneling attempts (which may indicate data leakage), and prevent misuse of the protocol, which may indicate potential threats and third-party software. It also provides protection against insider threats and vulnerabilities of applications and servers [27].



Geo Protection

Block network traffic to and from any country

Performance impact: Low

Profile: Default_Protection Action: Prevent

Policy for Specific Countries

Country	Action	Direction	Track	Comment
United Kingdom	Allow	From and To Country	Log	
United States	Allow	From and To Country	Log	

Policy for Other Countries

Block Track: Log

Policy Preview

Figure 6: Traffic control function in IPS (Geo-Protection)

This software has the ability to detect cyber attacks and anomalies and to provide real-time protection. It constantly updates the toolkit to counteract new threats, to which it is easily adapted. The toolkit is proactive and provides protection before vulnerabilities are discovered and exploits are created. Support and updating of this software is carried out only by its developers.

3.4 TippingPoing Next Generation Intrusion Prevention System

The TippingPoing NGIPS is a new generation product designed to prevent intrusions. It is used for network security and implements comprehensive protection against known and unknown vulnerabilities, prevents targeted attacks, blocks threats and malicious programs that are deployed or distributed in data centers and corporate networks. TippingPoing NGIPS is flexible and high-performance and integrates multi-generation protection technologies, including in-depth analysis of packages, threats, URL reputation and malware for client platforms and applications.

This product is designed for large-scale computer networks and has a high adaptability. The TippingPoint NX series (Figure 7-8) helps to reduce administration time and to prioritize network security with Enterprise Vulnerability Remediation (eVR), which allows customers to import vulnerability scanner data into the TippingPoint Security Management System and to pass them through service filters of digital vaccination Digital Vaccine and promptly to take appropriate action. The threat analysis implemented in the system provides the level of transparency that is necessary to optimize the state of information security throughout the organization [28].

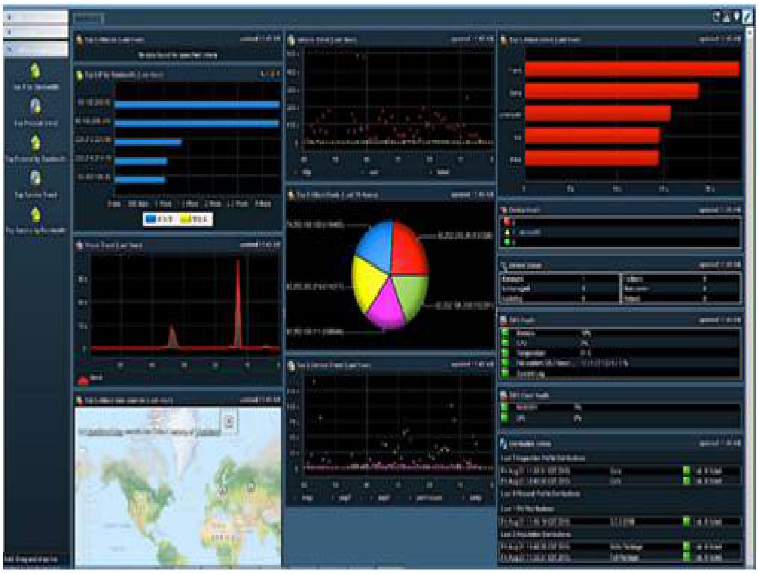
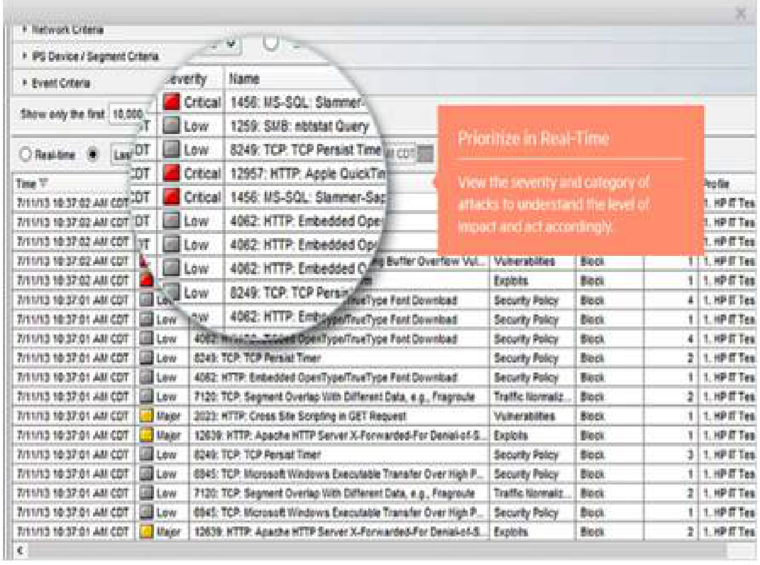


Figure 7: TippingPoint NGIPS information panel (real-time data scanning to find potential threats)



▸ Network Criteria

▸ IPS Device / Segment Criteria

▸ Event Criteria

Show only the first 10,000

○ Real-time ● Las

Severity	Name
Critical	1456: MS-SQL: Slammer
Low	1259: SMB: nbtstat Query
Low	8249: TCP: TCP Persist Time
Critical	12957: HTTP: Apple QuickTi
Critical	1456: MS-SQL: Slammer-Sa
Low	4062: HTTP: Embedded Ope
Low	4062: HTTP: Embedded Op
Low	4062: HTTP: Embedded O
Low	8249: TCP: TCP Persi
ow	4062: HTTP: Emb

Prioritize in Real-Time

View the severity and category of attacks to understand the level of impact and act accordingly.

Time ▽						Profile
7/11/13 10:37:02 AM CDT						1. HP IT Tes
7/11/13 10:37:02 AM CDT						1. HP IT Tes
7/11/13 10:37:02 AM CDT						1. HP IT Tes
7/11/13 10:37:02 AM CDT		g Buffer Overflow Vul...	Vulnerabilities	Block	1	1. HP IT Tes
7/11/13 10:37:02 AM CDT			Exploits	Block	1	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Lo	TrueType Font Download	Security Policy	Block	4	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	ype/TrueType Font Download	Security Policy	Block	1	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	4062: OpenType/TrueType Font Download	Security Policy	Block	4	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	8249: TCP: TCP Persist Timer	Security Policy	Block	2	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	4062: HTTP: Embedded OpenType/TrueType Font Download	Security Policy	Block	1	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Traffic Normaliz...	Block	2	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Major	2023: HTTP: Cross Site Scripting in GET Request	Vulnerabilities	Block	1	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Major	12639: HTTP: Apache HTTP Server X-Forwarded-For Denial-of-S...	Exploits	Block	1	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	8249: TCP: TCP Persist Timer	Security Policy	Block	3	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	6845: TCP: Microsoft Windows Executable Transfer Over High P...	Security Policy	Block	1	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Traffic Normaliz...	Block	2	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Low	6845: TCP: Microsoft Windows Executable Transfer Over High P...	Security Policy	Block	1	1. HP IT Tes
7/11/13 10:37:01 AM CDT	Major	12639: HTTP: Apache HTTP Server X-Forwarded-For Denial-of-S...	Exploits	Block	2	1. HP IT Tes

Figure 8: TippingPoint NGIPS operation in real time (mode of viewing the level of influence and categories of cyber attacks)

This software and hardware complex is focused on identifying misapplications and anomalies in the network, it adapts to new cyber attacks (contains adaptive intelligence), because it uses statistical models of machine learning and dynamic traffic analysis methods. This allows, based on the obtained network data, to make decisions in real time on the state of network security in order to protect it from new and complex attacks. Axoft invGUARD

The Axoft invGUARD software and hardware complex (developed by Axoft, Russia) monitors network traffic using the SNMP, NetFlow, BGP protocols and detects anomalies and network attacks. It consists of two basic components:

- a system for hardware and software complex for network traffic analysis (invGUARD AS);
- network traffic filtering and cleaning (invGUARD CS / CS-01).

Axoft invGUARD is focused on analyzing input data streams entering the IP through the network in order to detect DOS and DDOS attacks, BGP and SNMP anomalies, cyber attacks on the network infrastructure of broadcast packets and attacks on software applications.

The main functions of invGUARD include:

- continuous monitoring and analysis of traffic;
- cleaning incoming traffic using statistical and signature models;
- blocking external network attacks on the client network segments;
- ensuring the functioning of the client network segments with implemented security threats;
- centralization of control;
- the ability to scale and to adapt the complex to the features of the construction and the scope of the network;
- analysis of traffic of application protocols for blocking cyber attacks related to effects on the web interfaces and the application part of the information system;
- generating reports on various information (Fig. 9) [29].

The structural features of Axoft invGUARD allow effectively to detect misapplications and anomalies in the network. This is achieved through the use of methods of statistical, signature, heuristic, behavioral and dynamic analysis, which to a certain extent ensures the property of adaptability. The complex is closed and has ample opportunities to adapt to the network features. The system is controlled centrally and is aimed at collecting and analyzing network data and blocking cyber attacks. It is also possible to adapt and to scale by increasing the amount of traffic filtering tools. The structural features of Axoft invGUARD allow detection of attacks at the network and system levels [15]. The complex does not contain special protection mechanisms and reaction to the attack (or they are not disclosed by the developers) and works on Unixand Linux OS.

Defensepro. The DefensePro software and hardware tool (DefensePro DDoS Defense & DDoS Prevention Device, developed by RadWare, Israel) is designed to prevent network

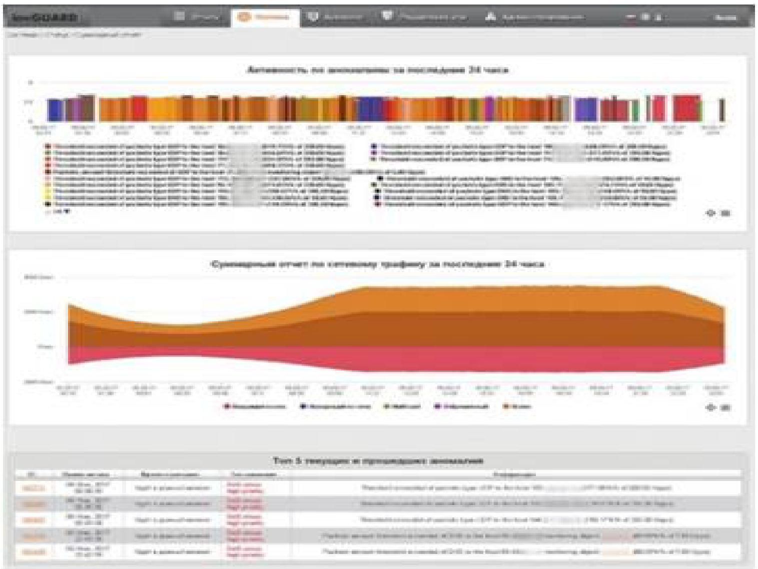
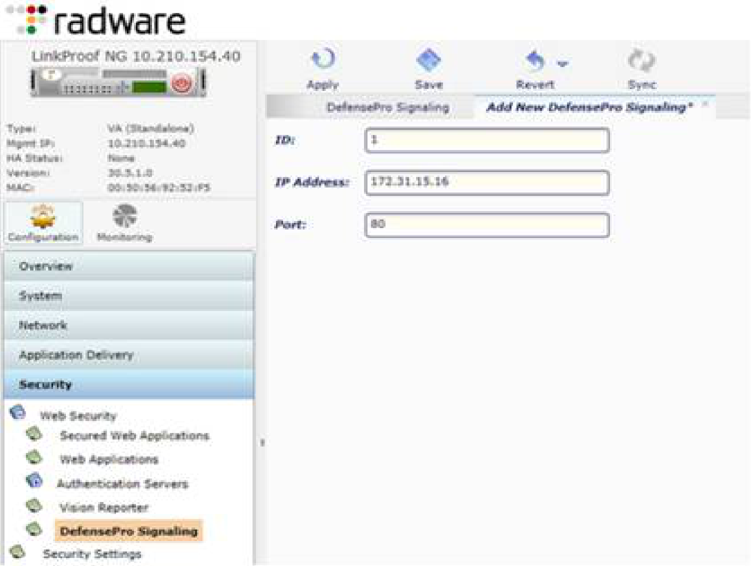


Figure 9: Axoft invGUARD system report window

intrusions and attacks in real time, which ensures the continuity of the network and applications (Fig. 10). It protects against the use of application vulnerabilities (application misuse), the spread of malicious software, network anomalies, malicious domains and IP addresses, information theft, Trojans and from DDoS (DoS) cyber attacks, spoofing, phishing, zero-day, SSL-based and authorization pages and CDN [17].



Type: VA (Standalone)
Mgmt IP: 10.210.154.40
HA Status: None
Version: 30.5.1.0
MAC: 00:50:56:92:52:F5

ID: 1
IP Address: 172.31.15.16
Port: 80

Figure 10: DefensePro software window

Two hardware components are included into DefensePro, the first of which is the DoS Mitigation Engine (DME), designed to repel massive DoS and DDoS attacks without affecting the normal traffic of a computer network, and the second one is the StringMatch Engine (SME), which accelerates signature detection characteristic of a particular computer network.

The complex also protects online services based on web applications and works with other security tools, which improves the security level of all services and applications.

Scalability is predetermined by a simple DefensePro system structure. The response module of the software and hardware complex to cyber attacks disconnects from the attacking object or blocks it. In combination with SSL Radware AppXcel, the specified complex provides a powerful and scalable solution for protecting against encrypted (SSL-based) attacks that can bypass continuous security controls. When an original SSL tunnel is formed between the client and the DefensePro server, it copies the SSL traffic to AppXcel, which decrypts it and sends it to the DefensePro for verification. When an attack is detected in the decrypted SSL traffic, DefensePro (in real time) blocks the malicious network connection.

The complex works in software emulators KVM kernel 3.19 (Unix, Linux), QEMU 2.0 (Unix, Linux, Windows, MacOS), VMware (ESX server versions: 5.1, 5.5, 6.0) (Unix, Linux, Windows).

KATA Platform. The KATA Platform system (Kaspersky Anti Targeted Attack Platform, developed by Avast, Russia) is designed to develop the latest technologies in the field of corporate computer networks and is used to protect against complex targeted attacks of any complexity. The KATA Platform solution integrates the latest technologies and global analytics, which allows to respond in a timely manner to targeted actions of the UAS and to resist attacks at all stages of their implementation. The software implements the functions of monitoring network activity, analyzing the behavior of objects in the system, identifying complex target cyber attacks and analyzing anomalies in computer networks [13].

In order to collect primary information about anomalies in the KATA Platform (Fig. 11), there are used sensors (special agents) that analyze IP, web and e-mail traffic and events on workstations and servers. KATA Platform agents are compatible with other software protection tools and have minimal impact on network and computer performance [14].

The KATA Platform operation is based on four stages and is a part of an integrated strategic approach in order to create an adaptive model of protection against new threats and to respond to information security incidents:

Stage 1 - Identification:

- continuous monitoring of activities that signal the start of an attack;
- detection of security vulnerabilities and network intrusion attempts;
- Incident detection, damage assessment and prioritization of further actions;
- training on targeted attacks investigation;
- reports on targeted attacks.

Stage 2 Response:

- malware analysis;
- operational counteraction to attacks and reduction of the harm connected with them;

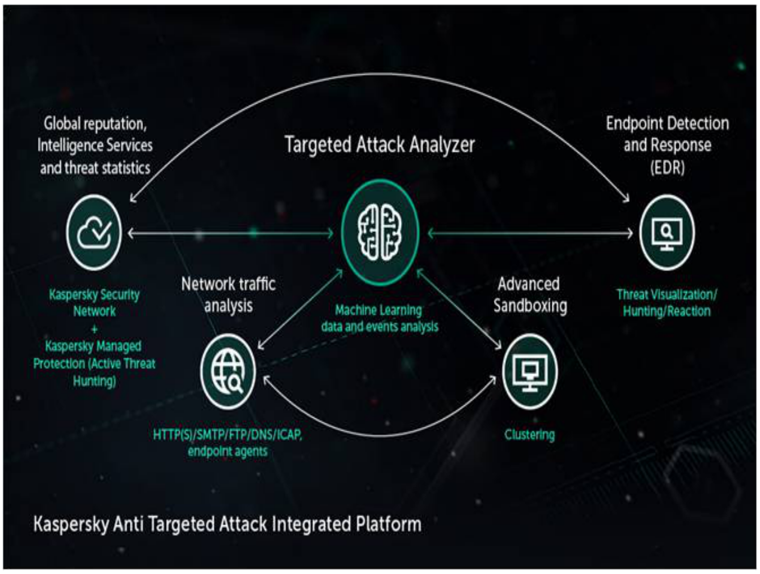

Global reputation, Intelligence Services and threat statistics
Targeted Attack Analyzer
Endpoint Detection and Response (EDR)
Kaspersky Security Network + Kaspersky Managed Protection (Active Threat Hunting)
Network traffic analysis
Machine Learning data and events analysis
Advanced Sandboxing
Threat Visualization/ Hunting/Reaction
HTTP(S)/SMTP/FTP/DNS/ICAP, endpoint agents
Clustering
Kaspersky Anti Targeted Attack Integrated Platform

Figure 11: Kaspersky Anti Targeted Attack Platform software window

- counteraction to incidents and their investigation;
- conducting deep digital criminalistics.

Stage 3 - Prediction:

- intrusion testing;
- assessment of the level of system security;
- assessment of potential security risks in the current infrastructure;
- recommendations for improving protection measures and addressing vulnerabilities;
- proactive protection that adapts to new and unknown threats.

Stage 4 - Counteraction:

- increasing employee awareness of current cyber threats (educational games, threat simulation, etc.);
- training on cybersecurity for professionals who increase the effectiveness of counteraction to the targeted attacks.

The KATA Platform is capable of detecting anomalies and complex targeted attacks of various kinds, and the constant and prompt updating of the database of network threats and the expansion of cyber-attacks detection capabilities allows users to be adaptable to new intrusions. Support and update of this software is provided only by the developer. Analysis of targeted attacks is carried out on the basis of information from network sensors, workstations and servers to create typical patterns of program behavior. Further, on the basis of deviations from these patterns, it is determined whether the activity is a potential part of a targeted attack. Also, suspicious objects detected in mail and Internet traffic transmitted by sensors into the sandbox, where each such object is analyzed for malicious activity, which allows detecting an attack at an early stage.

The system has centralized and distributed control, as well as the ability to adapt and to scale the platform to the amount of incoming traffic and network architecture. The structural features of the KATA Platform allow to detect cyber attacks at the network and system levels. Also, network sensors and workstations provide an opportunity to locate control points in different network segments and quickly to identify complex threats. The system responds quickly to attacks that it defines in the relevant database and enables digital criminalistics.

Special security mechanisms contained in the KATA Platform are not disclosed by the developers. The system operates on the basis of the OS Unix, Linux, Windows and MacOS.

Summary of IDS Analysis Results

4 Simulation Results

Cyber Attack Classes, Adaptability, Detection Methods, System Control, Scalability, Observation Level Response to Cyber Attack, Security, OS Support.

Table 1. Intrusion detection systems a summary of the results of the analysis

No	IDS	Classes of cyber attacks			Detection methods											System manage ment			Obser vation level				Support OS			
		Attacker	Anomalies	Adaptivity	Expert	Statistical	Signature	Scenario graphs	Event change control	Cluster	Dynamic	Machine-learning	Behavioral	Heuristic	Fuzzy sets	Centralized	Distributed	Scalability	System	Network	Response to a cyber attack	Security	Unix	Linux	Windows	MacOS
1	Shadow	+	+	-	-	-	-	-	+	-	-	-	-	-	-	-	+	+	-	+	-	+	+	+	-	-
2	Cisco IPS	+	+	+	-	+	+	-	-	+	-	-	-	-	-	+	+	+	+	+	+	+	+	+	+	-
3	Arbor Networks Spectrum	+	+	+	-	+	+	-	-	-	+	-	-	-	-	+	-	+	+	+	+	-	+	+	+	-
4	InfoWatch ASAP	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	+	-	-	+	+	+	+
5	Symantec DeepSight Threat Management System	+	+	+	+	+	+	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+
6	IPS	+	+	+	-	+	+	-	-	-	+	-	+	-	-	+	-	+	+	+	+	+	-	-	+	-
7	Tipping Poing NGIPS	+	+	+	-	-	+	-	-	-	+	+	-	-	-	-	+	+	+	+	+	+	-	-	+	+
8	Axoft invGUARD	+	+	-	-	+	+	-	-	-	+	-	+	+	-	+	-	+	+	+	-	-	+	+	-	-
9	DefensePro	+	+	+	-	+	+	-	-	-	-	-	+	-	-	+	-	+	-	+	+	+	+	+	+	+
10	KATA Platform	+	+	+	-	+	+	-	-	-	+	-	+	-	-	-	+	+	+	+	+	+	+	+	+	+

5 Conclusions

Analysis of misapplications and anomaly detection software systems, based on basic characteristics such as cyber attack classes, adaptability, attack detection methods, system control, scalability, system observation level, attack response, security, and supported OS, allows developers and users to choose the appropriate modern software in order to protect IS.

References

[1] Kornienko A.A., Slyusarenko I.M., "Sistemyi i metodyi obnaruzheniya vtorzheniy: sovremennoe sostoyanie i napravleniya sovershenstvovaniya [Systems and methods of intrusion detection: current state and areas of improvement]", *Moskva, CIT forum* (2009): 7-10.

[2] Mustafaev A.G., "Neyrosetevaya sistema obnaruzheniya kompyuternyih atak na osnove analiza setevogo trafika. Elektronnyiy resurs [Neural network system for detecting computer attacks based on network traffic analysis]", *Kaliningrad : ID «Yantarnyiy terem», Voprosyi bezopasnosti* No 2 (2016): 1-7.

[3] Branitskiy A.A., Kotenko A.V., "Analiz i klassifikatsiya metodov obnaruzheniya setevyih atak [Analysis and classification of network attack detection methods]", *Tr. SPIIRAN* No 2 (45) (2016): 207-244.

[4] Patel R., Thakkar A., Ganatra A., "A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems, *India : International Journal of Soft Computing and Engineering (IJSCE)* Vol. 2. Issue 1 (2012): 265-260.

[5] Al-Sakib Khan Pathan, "The State of the Art in Intrusion Prevention and Detection", *New York : Auerbach Publications* (2014): 516.

[6] Los A.B., Danielyan Yu.Yu., "Sravnitelnyiy analiz sistem obnaruzheniya vtorzheniy, predstavlennyih na otechestvennom ryinke [Comparative analysis of intrusion detection systems presented in the domestic market]", *Vestnik Moskovskogo finasovo-yuridicheskogo universisteta* No 3 (2012): 181-187.

[7] Akhemtov B., Korchenko A., Akhmetova S., Zhumangalieva N., "Improved method for the formation of linguistic standards for ofintrusion detection systems", *Journal of The oreticaland Applied Information Technology* Vol. 87, No. 2 (2016): 221-232.

[8] Belova A.L., Borodavkin D.A., "Sravnitelnyiy analiz sistem obnaruzheniya vtorzheniy [Comparative analysis of the detection systems]", *Sibir : SFU. Aktualnyie problemyi aviatsii i kosmonavtiki* Vol. 1, No 12 (2016): 742-744.

[9] Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md. Abu Naser Bikas, "An implementation of intrusion detection system using genetic algorithm", *International Journal of Network Security & Its Applications (IJNSA). Sylhet* Vol. 4, No. 2 (2012): 109-120.

[10] Lawal O.B. et al., "Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware", *African Journal of Computing & ICT. Ibadan* Vol. 6, No. 2 (2013): 169-184.

[11] Gamayunov D.Yu., Smelyanskiy R.L., "Sovremennyie nekommercheskie sredstva obnaruzheniya atak [Modern non-commercial attack detection tools]", *M.: F-t VMiK MGU. Programmnyie sistemyi i instrumentyi. Tematicheskiy sbornik* (2002): 20.

[12] Kuznetsov A.A. et al., "The statistical analysis of a network traffic for the intrusion detection and prevention systems", *Telecommunications and Radio Engineering. Kharkiv* Vol. 74, No. 1 (2015).

[13] Baboshin V.A., Vasilev V.A., "Obzor zarubezhnyih i otechestvennyih sistem obnaruzheniya kompyuternyih atak [Review of foreign and domestic computer attack detection systems]", *SPb : Sankt-Peterburgskaya nauchno-tehnicheskaya obschestvennaya organizatsiya «Institut telekommunikatsiy». Informatsiya i kosmos* Vol. 2 (2015): 36-41.

[14] Marjan Kuchaki Rafsanjani, Zahra Asghari Varzaneh "Intrusion Detection By Data Mining Algorithms", *Journal of New Results in Science. Tokat : Gaziosmanpasa University* No. 2 (2013): 76-91.

[15] Korchenko A.A., Ahmetova B.S., "Klassifikatsiya sistem obnaruzheniya vtorzheniy [Classification of intrusion detection systems]", *K.: NAU, InformatsIyna bezpeka* No 1 (13); No 2 (14) (2014): 168-175.

[16] Korchenko A.G. *Postroenie sistem zaschityi informatsii na nechetkih mnozhestvah* [The construction of security systems on the fuzzy sets] (K.: MK-Press, Teoriya i prakticheskie resheniya, 2006): 320.

[17] Cheswick B., "An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied" , *NY : Management Analytics and Others* (1997): 147.

[18] Andriy Dugin, "Cisco IDS/IPS. Bezopasnaya nastroyka [Cisco IDS/IPS. Secure configuration]" , *M. : OOO Izdatelskiy dom «Polozhevets i partneryi». Sistemnyiy administrator* No. 8 (81). (2009).

[19] "Arbor Networks Spectrum [Electronic resourse]" , *Tehnicheskie dannyie sistemyi Arbor. Burlignton : Arbor Networks Inc.* (2016): 4.

[20] "InfoWatch automation system advanced protector [Electronic resourse]" , *Zaschita ot atak na informatsionnuyu infrastrukturu ASU TP. Moskva : GK InfoWatch,* 2018.

[21] "IPS Software Blade contracts" , *SecureKnowledge Details : [website]. San Carlos : Check Point Software Technologies Ltd.* 2015.

[22] Northcutt Stephen, "Intrusion Detection: Shadow Style-Step by Step Guide" , *Dahlgren: SANS Institute* (1998).

[23] Mark Alexander Bain, "Build an IDS with Snort, Shadow, and ACID [Electronic resourse]" , *Security. San Francisco : The Linux Foundation* 2005. URL: https://www.linux.com/news/build-ids-snort-shadow-and-acid

[24] "Kaspersky Anti Targeted Attack (KATA) Platform" , *Kaspersky Lab : [website]. M.: AO Laboratoriya Kasperskogo* (2017). "Peredovaya platforma dlya zaschityi ot tselevyih atak i slozhnyih ugroz" , *Kaspersky Anti Targeted Attack Platform : [website]. Minsk : Gazeta Pravda* (2017).

[25] Kuznetsov A.A., "The statistical analysis of a network traffic for the intrusion detection and prevention systems" , *Telecommunications and Radio Engineering. Kharkiv* Vol. 74, No. 1 (2015).

[26] "HP TippingPoint Next Generation Intrusion Prevention System [Electronic resourse]" , *Geert Busse. Vilvoorde : Westcon-Comstor,* 2018. URL: http://be.westcon.com/content/vendors/hp-enterprise-security-solutions/hp-tippingpoint-ngips

[27] "SANS – Intrusion Prevention with TippingPoint [Electronic resourse]" , *Dave Shackleford. SANS Analyst Program. Swansea : SANS Institute by Trend Micro,* 2015. URL: https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/network/integrated-atp/SANS_TrendMicroTippingPoint2600NX.pdf

[28] "Kratkiy analiz resheniy v sfere SOV i razrabotka neyrosetevogo detektora anomaliy v setyah peredachi dannyih [Electronic resourse]" , *Habr : [website]* 2018. URL: https://habr.com/post/358200/

[29] Chi-Ho Tsang, Sam Kwong, Hanli Wang, "Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection" , *Pattern Recognition* Vol. 40, No 9. (2007): 2373-2391.

[30] Zadeh L.A., "Outline of a New Approach to the Analysis of Complex Systems and Decision Processes" , *IEEE Transactions on Systems, Man, and Cybernetics* Vol. SMC-3, No 1. (1973): 28-44.