Comparison of SGRC systems (Security Governance, Risk Management and Compliance)

Anton Lensky, Vladislav Vayts

We have prepared an overview and comparison of SGRC solutions presented on the Russian information security market. There are not many vendors working in this direction, so 5 "players" will participate in the review while the three of them are domestic.

First, we recall that the term SGRC stands for Security Governance, Risk Management and Compliance”. SGRC platforms, according to their names, solve the following problems:

- Governance - information security management with automation processes for asset management, vulnerabilities, documents, tasks, standards, as well as the ability to visualize the state of information security and create reports.
- Risk Management - cyber risk management with automation of a risk-based approach to information security aimed at an economically justified choice of optimal security measures that minimize the identified and calculated risks.
- Compliance - ensuring compliance with legislation, industry and internal standards and requirements (compliance), with the ability to conduct audits and provide reports and results.

Additionally, SGRC systems can perform the following functions:

- managing internal documents, knowledge base and solutions, performing the "internal Wiki" function for information security departments;
- managing a variety of business processes related to information security;
- managing the processes of interaction with counterparties on information security problems;
- reporting and visualizing the state of information security as interactive graphs and diagrams;
- providing integration with the OS, software, and SPI to obtain information about the state of the infrastructure components;
- support for information security incident handling;
- support for managing business continuity and recovery processes;
- providing management decision-making support for management (situational awareness).

Classic business-oriented GRC systems focus on broader categories of management processes and risks than any specialized SGRC solutions. However, the specialization of SGRC products in cybersecurity brings additional functionality to solutions, such as automation of response to information security incidents, interaction with security tools, and special reporting.

The review presents the main players on the SGRC systems market:

- ePlat4m (Russia)
- Microsoft 365 Compliance Center (USA)
- RSA Archer (USA)
- R-Vision (Russia)
- Security Vision (Russia)

We will compare and analyze these solutions according to their general, technical and functional characteristics and capabilities, making conclusions after each section.

Comparison criteria	ePlat4m	Microsoft Compliance Center	RSA Archer	R-Vision	Security Vision
1. Comparison of general and technical characteristics					
1.1. Software requirements					
Version	1.8.6	June 2020	6.8	4.4	4.1.7
Delivery option	On-premise and SaaS installation	Cloud solution (SaaS) on Microsoft Azure	Installation on-premise and on Amazon Web Services, Microsoft Azure	Software appliance, it is possible to deploy on physical servers. In case of low estimated loads, there is an option to place all components in the All-in-one mode (on one server).	Software appliance, it is possible to deploy on physical servers. In case of low estimated loads, there is an option to place all components in the All-in-one mode (on one server).
Virtualization environments	No	Cloud solution (SaaS)	VMware	VMware, VirtualBox, Hyper- V, Xen, Parallels	VMware, VirtualBox, Hyper- V, Xen, Parallels, KVM
Solution components	DBMS server, webserver	Cloud solution (SaaS)	DBMS Server, Web Server, Service Server	Management server, DBMS server (can be combined with the management server), central collector, inventory collector.	Management server, DBMS server, connector services (connectors to data sources and response connectors), monitoring service.
OS	Microsoft Windows Server 2012 and later	Cloud solution (SaaS)	Microsoft Windows Server 2012R2/2016	Management server, collectors: CentOS 7, RHEL 7, Astra Linux CE 2.12, AltLinux Alt 8 SP. DBMS Server: Ubuntu 14/16, CentOS 7, RHEL 7, Windows Server 2012/2016, FreeBSD 11	Management server, connector services, monitoring service: Microsoft Windows Server 2012R2 and later, CentOS 7 and later, RHEL 7 and later, Ubuntu 14 and later, Astra Linux CE, AltLinux, Alt. DBMS Server: Microsoft Windows Server 2012R2 and later, CentOS 7 and later, RHEL 7 and later, Ubuntu 14 and later, FreeBSD 11 and later, Astra Linux CE, AltLinux, Alt.
DBMS	MS SQL 2012 and later, PostgreSQL	Cloud solution (SaaS)	MS SQL 2016	PostgreSQL v10 and later.	PostgreSQL 9.5 and later, MS SQL 2014/2016 and later
Customer software	Web browser	Web browser (Google Chrome, Mozilla Firefox, Internet Explorer, Edge)	Web browser (Google Chrome, Mozilla Firefox, Internet Explorer, Edge)	Web browser (Google Chrome, Mozilla Firefox, Internet Explorer)	Web browser (Google Chrome, Mozilla Firefox, Internet Explorer, Edge, Yandex)
1.2. Customer hardware and infrastructure requirements					
CPU architecture		Cloud solution (SaaS)	Any that supports the server OS.	x86	Any that supports the server OS.
Hardware	8 CPU 8 GB RAM	Cloud solution (SaaS)	No data available	Depending on the number of assets, response scripts, system users: Management server: 1- 22 CPU 8 - 32 GB RAM DBMS server: 1 - 16 CPUs 8 - 24 GB RAM	Management server: 1-12 CPUs 4-16 GB RAM DBMS server: MS SQL / PostgreSQL: 1-16 CPU 4-32 GB RAM Connector services, monitoring

				Collector (recommended parameters): 4 CPU 8 GB RAM	service: 1-2 CPUs 2-4 GB RAM
Support for distributed component placement (geographically distributed sites, isolated LAN segments)	No data available	Cloud solution (SaaS), servers are distributed worldwide	No data available	Yes	Yes
Optimization of the footprint on the customer's IT infrastructure during the operation of the solution components	No data available	Asynchronous task execution	No data available	Algorithms for optimizing network scanning and reducing the load on the LAN	Algorithms for optimizing network scanning and reducing the load on the LAN, scanning parallelization, separation of scanning depth levels
Ability to install solution updates via the Internet	No data available	Yes	Yes	Yes	Yes
The ability to install updates without Internet access	No data available	No	Yes	Local update available	Yes
1.3. Ease of use and administration					
Documentation	Provided as pdf documents	Available on the Microsoft website	Provided as pdf documents	Provided as contextual HTML help and as a separate document.	Provided as contextual HTML help and as a separate pdf document.
Documentation language	Russian	English, Russian (machine translation)	English	Russian	Russian
Interface language	Russian	English, Russian (not all menu items can be translated from English)	English	Russian, English	Russian, English, multilingual support (the ability to add any languages).
Design themes	Not supported	Light, dark.	Not supported	Light, dark.	Light, dark.
Granted access rights to the OS on which the solutions are deployed	Administrator	Restricted by Tennant	Administrator	Root (full)	Administrator/root (full)
Solution user authentication	Domain authentication	Authentication via Azure AD	Domain authentication (NTLM, Kerberos), built-in	Domain authentication (NTLM, Kerberos), built-in authentication.	Domain authentication (NTLM, Kerberos and including SSO), Radius

methods			authentication.	Note: domain authentication requires preliminary configuration using the Linux terminal, since the management server is running Linux.	authentication, built-in authentication. Note: Support for assigning roles to system users based on group memberships in Active Directory.
Configuring networking	The final list of required protocols and ports.	The final list of required Internet addresses, protocols and ports. The list of Internet addresses may be updated	The final list of required protocols and ports. Typically, TCP:443 is used everywhere	The final list of required protocols and ports, iptables configuration is done using the Linux terminal.	The final list of required protocols and ports, the configuration of the Windows firewall is done using the GUI or command line. The iptables configuration is done using the Linux terminal.
Configuring the display of information	Depending on the user's rights and role	Depending on the user's rights and role	Depending on the user's rights and role	Ability to select items from the list of available elements, sort data, and save customized filters	Fully customizable workspace for a role, preset filters and display parameters, the ability to customize the composition of displayed elements, filtering while saving settings, sorting by all data, additional functionality for complex sorting by all data
Search for all objects from a single interface	Search for all elements	Search for all elements	Search for all elements	Search for all elements, incl. linked.	Global search for all objects.
Import, export of solution items	Export as docx, xlsx, pdf	Some items are exported as csv	Import/export of data as xml, xls	Import data about assets (such as Organizations, Equipment, Networks), Audit evaluation results, Audit requirements, and a list of items from Excel spreadsheets (a file with a specified template). Export asset data, list of items, tasks, guides (optional), reports, threat models, and system logs as xlsx, docx, and pdf. Export map elements, diagrams to a graphical format (png). Export and import of connector data as json	Import/export any data in machine-readable form. Export of reports as xlsx, csv, docx, pdf. Import / export any objects as xlsx, csv, docx, pdf. Import/export of customized workflows in internal format. Export elements to a graphic format (png, jpeg).
User notification options	Sending email	Sending email, pop-up notifications in the web interface	Sending email	Sending email	Sending email, SMS, Telegram notifications, audio alerts, and pop-up notifications in the web interface
Configuring alerts	Partial notification configuration	Partial notification configuration	Partial notification configuration	Automatic generation of reports on a schedule, sending notifications to	Ability to configure arbitrary custom events to notify about changes in

				responsible persons (users, roles) for a certain type of assignment (task, vulnerability, remark or audit check), sending a notification about the occurrence of a certain event in the system (users, assets, vulnerabilities, audits)	monitored properties of objects, setting conditions for triggering notifications (depending on the properties of monitored objects). Full configuration of the notification text, using the attributes of the object that the notification is being sent for
Personal API	No	Azure REST API	RESTful API Web API Personal GRC API	REST API	REST API
1.4. Differentiation of access rights to the system					
Access control model	Role-based access control Discretionary access control model	Role-based access control	Role-based access control	Role-based access control System roles: access to sections of the system for reading or changing, for example: Administrator, User, Risk Manager, etc. Special roles: access to individual elements of the system, for example: Asset owner, Security administrator, Security auditor, etc.	Role-based access control Customizable roles based on object attributes Differentiation of access to all system objects and the assignment of rights to read, modify, create, perform group operations for a specific user / group. Permissions are built on the "Module – Access Object – Access Right – Policy" principle
Granular access support	No data available	Yes	Yes	The ability to create custom roles with permissions to perform certain actions with certain objects, group users, and assign them roles	The ability to create custom roles with permissions to perform certain actions with certain objects, group users, and assign them roles. The ability to restrict access to view certain properties of specific objects (for example, certain properties of incidents containing confidential information). The "Workflow" functionality allows defining the order of interaction with any logical object (incident, asset, vulnerability, task, etc.) of various user groups, including those depending on the current state and values of the object's properties, taking into account the roles and rights of users

1.5. Logging					
Log of user actions	The history of actions of users and administrators is logged.	The history of actions of users and administrators is logged	The history of actions of users and administrators is logged	The history of actions of users and administrators in all modules is logged, including the export of log data and sending it via syslog.	The history of user and administrator actions in all modules is logged, including sending activity information to email, syslog, and SNMP.
Logging actions with objects	Yes, user and system actions	Yes, user actions	Yes, user and system actions	The history of changes to all elements is logged (changing the value of fields, actions with elements, adding objects).	The history of changes to all elements is logged (changes in properties, states of the workflow, completed transactions) with the preservation of the old and new value of the changed property
Monitoring solution performance	Logging by means of OS	Logging by means of the system	Logging by means of the system	Logging by means of OS (text files), logging by writing events to the database.	Logging by means of OS (Windows Application log, text files), logging by writing events to the database.
Solution security log	OS system log	History of user logins and logouts, failed login attempts, account lockouts, access rights changes, user list changes, password changes	History of user logins and logouts, failed login attempts, account lockouts, access rights changes, user list changes, password changes	History of user logins and logouts, failed login attempts, account lockouts, access rights changes, user list changes, password changes	History of user logins and logouts, failed login attempts, account locks, access rights changes, user list changes, password changes, list of IP addresses from which the connection was made
1.6. Security					
Secure communication between solution components	Use of the SSL/TLS protocols	Use of the SSL/TLS protocols	Use of the SSL/TLS protocols	The use of the SSL/TLS protocols and ability to authenticate with certificates between all system components, the use of certificates issued by a Certificate Authority (CA). Note: PKI is configured using the Linux console	The use of the SSL/TLS protocols and ability to authenticate with certificates between all system components, the use of certificates issued by a Certificate Authority (CA)
Protecting user access to the web interface	Access to the web interface via HTTPS	Access to the web interface via HTTPS	Access to the web interface via HTTPS	Access to the web interface via HTTP/HTTPS, using the TLS 1.2 protocol	Access to the web interface via HTTPS, using the TLS 1.2 protocol, the ability to restrict the IP addresses that are allowed access
Setting the web session timeout	No data available	Yes	Yes	Yes	Yes
Setting password complexity and expiration (when using built-in	No data available	Yes	Yes	Yes	Yes

authentication)					
Account lockout in case of unsuccessful authentication attempts	No data available	Yes	Yes	The blocking algorithm is configurable	The blocking algorithm is configurable
Two-factor user authentication	No data available	Yes, SMS, OTP	No data available	Yes, according to certificates	Yes, according to certificates
Restricting access to the solution at the network level	No data available	By restricting access to the MS Azure tenant	By means of MS IIS server	No (via iptables manually via the Linux console).	Yes, via the web interface: permission to access the system only from certain IP addresses, IP address ranges, subnets.
Mail gateway authentication	No data available	Yes	No data available	Support for SSL connection, authentication on the mail server	Support for SSL connection, authentication on the mail server
1.7. Licensing					
License cost	Depends on the number of functional modules, connectors to external ISs	According to MS Office 365 price list with the E5 plan	No data available	It depends on the functionality, total number of assets, number of users, number of connectors, customization of the solution for a specific Customer, and duration of the purchased technical support.	It depends on the list of selected functional modules, the number of connectors to data sources and response connectors, the ability to use high availability/multithreading mode, and the selected level of technical support
License type	Indefinite	Subscription	No data available	Indefinite	Indefinite, limited
Licensing verification tool	No data available	Online verification of subscription validity	No data available	The license is installed as a file associated with a unique installation ID	The license is installed as a text key generated based on the unique installation identifier
According to the SaaS model	Yes	Yes	No data available	No	No
Technical support	Depending on the level purchased: 8x5 (GMT+5) Service language: Russian	Yes Service language: Russian, English.	No data available	It includes receiving periodic updates, providing advice on the use of the software product, and 24/7 support. Service language: Russian, English	Depending on the level purchased: 8x5 or 24/7, fault response time from 8 to 2 hours, provision of patches, free upgrade to new versions. Service language: Russian, English
Extra		The solution is delivered as part of an MS Office 365 subscription with the E5 plan	No data available	Expertise packages, sets of audit requirements are purchased separately	The vendor offers both "box" and completely customizable for a specific customer
1.8. Certificates					
Certificates	The product is included in the Unified Register of Russian Programs for Electronic Computers and Databases.	No	No	FSTEC Certificate of Conformity No. 4346 dated 22/12/2020, can be used in significant objects of CII category 1, APCS-1, GIS-1, ISPDn-1 and in public	FSTEC Certificate of Conformity No. 4194 dated 12/19/2019, can be used in significant objects of CII category 1, APCS-1, GIS-1, ISPDn-1 and in

				information systems of class II. The product is included in the Unified Register of Russian Programs for Electronic Computers and Databases.	public information systems of class II. The product is included in the Unified Register of Russian Programs for Electronic Computers and Databases
1.9. Deployment (list of Customers according to open sources)					
Deployment	No data available	No data available	PJSC "Rosbank"	JSC "RSHB", VTB Bank (PJSC), PJSC "MTS-Bank", JSC "Russian Railways", Bank GPB (JSC), Federal Tax Service of Russia, JSC "SO UPS"	PJSC Sberbank, State Corporation "Rostec", PJSC Bank "FC Otkrytie", JSC "Goznak", The «General Radio Frequency Centre» Federal State Unitary Enterprise (FSI)", FSO of Russia, FAU Glavgosexpertiza of Russia, SDM-Bank (PJSC), Gazprom-Media Holding JSC
1.10. Other					
Working in the multitenancy mode	No data available	Yes	No data available	Yes, support for access control and role model for MSSP without physical data separation	Yes, with support for granular access control for MSSP
Fault tolerance	Yes	Yes	No data available	Yes, in the Active-Passive, Active-Active modes	Yes, hardware duplication of all system components, software distribution of tasks to ensure fault tolerance and load balancing

Conclusions on Section No. 1

EPlat4m and RSA demonstrate a level of customization, service and support that is typical for business products, if we do not take into account the difference in the country of origin and the potential cost of the solution.

The ePlat4m product is not yet widely used. However, we would like to note that it has a certificate of compliance with the FSTEC of Russia, which is an indisputable competitive advantage, and also indicates the necessary security features implemented in the product. Therefore, it is quite correct, in our opinion, to talk about the existence of positive prospects for the implementation of this product on the Russian market, especially among government agencies.

The RSA solution is also not being sold very actively in Russia. In addition, it is "tuned" for integration in the ecosystem of products from RSA and has a few cases of implementations in Russia.

Similarly, the solution from Microsoft is focused on working in the MS Azure stack and is, like other Azure solutions, cloud-based, which imposes restrictions on the list of potential buyers, given the strict legal requirements.

The R-Vision solution is actively spreading on the market. It is based on the Linux OS, which, as a result, leads to the need for the customer's staff with the necessary *NIX competencies (working in the command line, configuring Linux system utilities). At the same time, once set up, such a solution is likely to show a long Uptime.

The Security Vision product is in demand on the Russian market. Among the systems we are reviewing, only it and ePlat4m are certified by the FSTEC of Russia. Security Vision can operate in a Windows environment familiar to the average user, which simplifies the configuration process (for example, it is easy to integrate it into the current Microsoft Active Directory environment), and also somewhat reduces the requirements for the competencies of the employee administering this system. Security Vision supports Open Source installations based on Linux OS and PostgreSQL DBMS, which reduces the financial requirements for the customer's IT infrastructure.

In terms of ease of use and administration, the most attractive are Microsoft Compliance Center, R-Vision and Security Vision. The documentation for the R-Vision solution looks solid, and the contextual help with search is also convenient. Microsoft Compliance Center and Security Vision have documentation not only in Russian, but also in English, as well as multilingual technical support.

Security Vision offers the greatest variety of notification types: sending email, SMS, Telegram notifications, audio alerts, and pop-up notifications in the web interface. EPlat4m, RSA Archer, and RVision only support email notifications, while Microsoft Compliance Center supports email notifications and pop-up notifications in the web interface.

In terms of certification, it is quite natural that domestic products are in the lead. All three Russian systems under consideration - ePlat4m, R-Vision and Security Vision - are included in the Unified Register of Russian Programs for Electronic Computers and Databases. R-Vision and Security Vision have the FSTEC of Russia certificates of conformity.

2. Comparison of functionality **2.1. Information Security Management**					
2.1.1. Inventory and asset management					
List of supported asset types	Tangible and intangible assets: • processes • information • systems • networks • equipment • users	Tangible and intangible assets: • information • systems • equipment • software • vulnerabilities • users	Tangible and intangible assets: • information • systems • equipment • software • vulnerabilities • users	Two asset classes (business assets and IT assets), but new asset types can be defined within each class. Preset asset types: • Organization (entities) • Business processes • Information • Staff • Premises • Network equipment • software • Domains • Vulnerabilities • Groups of IT assets (information systems)	Any types of assets. Working with assets is configured through the universal functionality of workflows that implement the tool for processing and the life cycle of logical objects, including assets. A graphical editor for the workflow designer is provided. Preset asset types: • Buisness process • Information system • Technical mean • software • License • Information
List of supported asset types	No data available	Asset properties are not customized	No data available	Asset properties are defined in guides. Personal elements can be added to guides. Adding a new guide is not supported. About 10 types of directories are preset (asset types, security attributes, business processes, information assets, equipment types, etc.)	Arbitrary asset properties, custom properties are supported. The link of asset properties with the elements of guides and knowledge bases is supported. Property types: time interval, date/time, employee group, yes/no, fractional/integer, text / extended text (with HTML markup support), linked assets, employees, file, guide

Links between assets	Yes	Yes, links between hardware, software, users, vulnerabilities	Yes	Linking between asset types: equipment, groups of IT assets, business processes, information. Linking ("Affects" or "Depends on") security attributes (integrity, confidentiality, availability) between assets. There is an asset classifier with the ability to automatically categorize assets according to applicable regulatory requirements. Assets are linked to the "Audits" module - the asset property contains a link to the audits performed, violations of requirements on the asset and equipment, premises, system, as well as a work plan to eliminate violations. Assets are linked to the "Risk Management" module and the categorization of the object as part of the CII protection requirements. Fast transition from an asset to its hardware, applicable standards/requirements, incidents (IRP functionality) is supported	One can configure the types of links ("Linked" or "Depends on") between any types of objects. The interaction between assets is configured through the universal functionality of workflows that implement the tool for processing any logical objects, including assets. Ability to link assets with any types of objects in the system: documents, files, legal requirements, tasks, incidents (IRP functionality), etc. It supports monitoring changes in the properties of linked assets with automatic actions performed when user-defined conditions occur
The amount of collected and inventory information about the equipment (built-in solution tools)	No data available	• Device name • IP address • MAC address, number of network interfaces • OS type • Type of equipment • Domain name • Hardware specifications (CPU, RAM, Hard Drive) • Installed software (version) • List of domain users • OS security options • Vulnerabilities	No data available	• Device name • IP address • MAC address, number of network interfaces • Subnet mask • OS type • Hardware type (depending on the type of software installed), role (in the case of Windows server OS) • Physical /virtual machine • Domain name / working group • Hardware specifications (CPU, RAM, Hard Drive) • Installed software (version,	• Device name • IP address • MAC address, number of network interfaces • Subnet mask • OS type • Type of equipment • Physical /virtual machine • Domain name / working group • Hardware specifications (CPU, RAM, Hard Drive) • Installed software (version, date of installation) • List of local/domain users/ administrators

				date of installation) • List of local / domain users / administrators (username, last login date) on the device • List of domain security groups included in local security groups on the device • OS security settings (antivirus status with version indication, firewall status, OS update service status, USB device connection options) • Vulnerabilities (by integrating with a third-party solution - vulners.com) • Additional fields for manual entry (asset status, responsible persons, inventory number, etc.)	• List of domain security groups included in local security groups on the device • OS security options • Vulnerabilities • Additional fields for manual input
Functionality of built-in inventory tools	No data available	Agent inventory is carried out using the Microsoft Defender ATP, SCCM client installed on the device	No data available	• Agentless inventory is carried out by the R-Vision collector: scanning a given network using nmap, followed by remote login to the device (WMI, MS RPC for Windows systems; SSH/SNMP for Linux/Unix systems, Cisco, Juniper, HP network equipment) • Execution of proprietary scripts (such as R-Vision) on collectors to automate actions for collecting inventory information • Running local VBScript logon scripts on devices inaccessible for remote login, and then sending the collected data in a POST request to the collector • Universal connector for integration with arbitrary databases of MS SQL, Oracle, Postgresql types, data import from an arbitrary Excel table	• Agentless inventory is carried out by the Security Vision data collection connector, which supports the following protocols and mechanisms: DNS, HTTP, HTTPS, IMAP, MS RPC, POP3, SMTP, SNMP, SSH, SSL, Syslog, TLS, WindowsShell, WMI; tools for connecting to directory services Active Directory and DBMS Microsoft SQL, MySQL, Oracle, PostgreSQL; API tools (REST, SOAP) • Universal Security Vision connector, • that connects to virtually any system capable of providing machine-readable data • The data deduplication algorithm is flexibly configured according to logical rules (comparison of event properties) • The tool for configuring

				• The collected data on user permissions on devices is aggregated in the "User Privileges" guide • Ability to set custom software groups with different software assigned to them by using regex expressions • Search for installed software in user-defined guides • Scanning for detected subnets linked with the network adapters of the inventoried devices • Asset deduplication algorithm (takes into account the uniqueness of MAC, UID, the presence of a token file on the scanned system)	filtering and grouping rules allows customizing any logic for selecting, linking and grouping the received information about scanned assets • Ability to monitor network accessibility, the quality of communication with devices and the status of assets (using ICMP, TCP, UDP, SNMP, Syslog) with the visualization of the received data on graphs • Ability to remotely log in to the scanned equipment (via RDP, SSH) • Response Connector Managers can automatically distribute tasks among themselves to ensure fail-safety and load balancing during the inventory process.
The amount of collected and inventory information about equipment (based on data from connected systems)	The amount of data depends on the specific source system	• Installed software (version, number of installations, licenses, license validity period) • Hardware specifications • Vulnerabilities	The amount of data depends on the specific source system	• Installed software (version, number of installations, licenses, license validity period) • Hardware specifications • Vulnerabilities • Users (domain): full name, account name, position, entity, data when the awareness programs were passed • Status of information protection tools on devices (status of DLP agents, antiviruses, anti-tampering tools, etc.)	The amount of data depends on the specific source system. Examples of popular sources can be found below: Kaspersky Security Center: Network name, network address, anti-virus server, domain, last available time, last update time, last scan time, anti-virus group, node visibility, agent installation status, agent launch status, protection service status in real time, OS platform, number of detected malware, number of untreated malware, processor architecture, last boot time, operating system, version and name of the antivirus, signature database update date. MaxPatrol 8: network address, network name operating system, installed software, software versions, software installation path, complete information on all vulnerabilities. MS SCCM: Network address, IDs, domain, network name, operating

					system, MAC address, auto-update activation status. The above list is not final: other sources-systems transmit their lists of data to the system
Configuring the inventory process	No data available	Automatic scanning, on-demand scanning	No data available	Configuring the launch of automation scripts (target group of devices, launch schedule). Configuring the attribute assignment policy - the logic for filling in the properties of detected assets (for example, linking a device with an information system, grouping assets according to specified criteria). Configuring software detection policy (searching for specific files and directories on devices). Configuring scan policies (schedule, used accounts, scanned LAN subnets). Configuring the personnel security policy - building a map of the" vulnerabilities" of employees depending on the results of training phishing attacks and employees' training in the "Antiphishing" system	The inventory process is flexibly configured as part of a logical inventory workflow. There are manual (performing actions at the user's command) and automatic (performing actions when certain conditions occur) transactions-actions on the target system that are configured as part of the inventory workflow using a graphical editor. The actions include creating a new object, changing the properties of the current object, filling guides, executing automation scripts (Bash, PowerShell, Batch, cmd, Java, Javascript, Python), executing queries to systems (SNMP, SOAP, REST, DNS), and executing queries to databases (MS SQL, MySQL, Oracle, PostgreSQL). There is a chat on objects, in which users of the system can communicate on tasks linked to the asset.
Integration with third-party solutions	MaxPatrol 8 MaxPatrol SIEM Micro Focus ArcSight ESM RedCheck Tools: RDBMS (ODBC, OLEDB) SOAP WS REST WS LDAP POP3/SMTP XML (file) MS EXCEL (file)	Aruba ClearPass Policy Manager AttackIQ Platform Azure Sentinel Better Mobile BitDefender Blue Hexagon Corrata CyberMDX CyberSponse CyOps Cymulate Cyren Wen Filter Delta Risk ActiveEye Demisto IBM QRadar Lookout MTP Micro Focus ArcSight	MaxPatrol 8 Micro Focus ArcSight ESM Nessus Qualys RSA Netwitness SIEM, other RSA products Symantec SIM	Active Directory AlienVault Atlassian JIRA Cisco (SSH, REST) CMDB iTop Forcepoint AP-DATA Fortinet FortiMail Fortinet FortiSandbox Gigamon GigaVue-Fm Group IB Bot-Trek Intelligence HP Comware HP SM (REST) IBM QRadar Imperva InfoWatch Device Monitor InfoWatch Traffic Monitor Juniper	Active Directory Apache Kafka Atlassian Confluence Atlassian JIRA Cisco (SSH, REST, SNMP) Cisco FirePower Cisco IronPort/ESA CMDB iTop CheckPoint CheckPoint SandBlast FireEye FireEye IPS Fortinet FortiMail Fortinet FortiSandbox Fortinet SIEM Gigamon GigaVue-Fm HP SM (REST, SOAP)

		ESM MISP ThreatSharing Morphisec Nexpose Rapid7 Palo Alto RSA Netwitness SIEM SafeBreach ServiceNow Skybox Splunk Swimlane Symantec Endpoint Protection Mobile THOR Cloud ThreatConnect Vectra NDR XM Cyber Zimperium		Kaspersky Fraud Prevention Kaspersky Security Center Lieberman ERPM MaxPatrol 8 MaxPatrol SIEM McAfee ePO McAfee ESM Micro Focus ArcSight ESM Micro Focus UCMDB MS Exchange PowerShell MS SCCM MS SQL MS System Center Endpoint Protection MS TMG MySQL Naumen CMDB Naumen Service Desk Nessus Nexpose Rapid7 OpenStack OpenVAS Oracle DB Palo Alto PostgreSQL QLikView Qualys RedCheck Secret Net Secret Net Studio Solar JSOC Splunk StoneGate Symantec Endpoint Protection VMware Vulners.com Zabbix Anti-phishing Note: When integrating with Active Directory, limited account properties are collected (full name, account name, position, entitity), and it is not possible to configure getting the values of other properties.	HP SM ADV IBM MQ IBM QRadar (REST) Imperva SecureSphere InfoWatch Traffic Monitor Juniper Kaspersky IPS Kaspersky Security Center Lieberman ERPM MailArchiva MaxPatrol 8 MaxPatrol SIEM McAfee ESM Micro Focus ArcSight ESM MS Exchange PowerShell MS SCCM MS SQL MS System Center Endpoint Protection MS TMG MXtoolBox MySQL Naumen Service Desk Nessus OpenStack Oracle DB OTRS Palo Alto IBM QRadar PostgreSQL QLikView Qualys RedCheck RSA Netwitness SIEM RuSIEM ScanOVAL Skybox (REST, SOAP) Splunk Symantec Critical System Protection Symantec Endpoint Protection Symantec IPS TripWire URLScan.io VirusTotal VMware ESXi

				The data received from integrated systems is limited by the status of the IST, the technical characteristics of the devices, the list of devices, users, software, and vulnerabilities. Connecting a new system takes from 1 day	VMware vCenter Zabbix 1C AS Bank State Internet services (FSSP, USRIE, EGRIP, etc.) CIB SearchInform Consultant + Subsidiaries and affiliates portal ACS (various developers) SPARK-Interfax FPSU-IP FPS-TLS Note: From the connected systems, one can receive, process, normalize, and upload to Security Vision any data that the target system can provide, including unstructured data (XML, JSON, CSV, TXT, Binary). Requests to external public services (Google API, Yandex API) are supported. Connecting a new system takes 1-2 hours
Required access rights for collecting inventory data	**No data available**	Agent inventory	No data available	To scan Windows systems, one must grant the account local administrator rights on the target device.	To scan Windows systems, one must grant the account local administrator rights on the target device. It is possible to use standard domain user permissions to connect to Active Directory
Metrics of the asset inventory process	**No data available**	Visualizing vulnerability elimination, application of recommended security settings, information security status (Security Score, Compliance Score) as diagrams	No data available	Metrics types: incident response time (IRP functionality), response time compliance, damage incurred and prevented. The creation of additional custom metrics is not supported. Metrics are maintained for assets of the type "Organization" ("Entities"), "Business Processes", "Groups of IT Assets".	Any required metrics, setting custom algorithms and comparison logic, and custom thresholds. Creating metrics for any type of entity, including assets. Visualization of metrics: as interactive charts and dashboards with the Drill-Down function, graphs, reports

				Modifying thresholds for metrics and setting personal metrics for specific assets are supported. Visualization of metrics: graphical (graphs, color indication) and digital (text) views	
2.1.2. Vulnerability Management					
Sources of information about vulnerabilities	Integration with vulnerability scanners	Personal repository, MITER repository	Integration with vulnerability scanners	The data obtained from the inventory on the installed software is correlated with the vulnerability database - Vulners.com, which aggregates data from various vulnerability repositories (CVE, vendor databases). Integration with BDU FSTEC of Russia. Integration with vulnerability scanners	Integration with BDU FSTEC of Russia, ScanOVAL software. Integration with vulnerability scanners. Integration with any repository of vulnerabilities is possible
Vulnerability severity criteria	It meets criteria used by vulnerability scanners	It conforms to the CSS v3 notation	It meets criteria used by vulnerability scanners	Personal criticality metric - R-Vision (5 levels)	Flexibly configurable. By default, it conforms to the CSS v3 notation
Types of vulnerabilities	• Software vulnerabilities	• Software vulnerabilities • Configuration vulnerabilities	• Software vulnerabilities	• Software vulnerabilities	• Software vulnerabilities • Configuration vulnerabilities
Vulnerability data	No data available	No data available	No data available	• Vulnerability description • Source • Severity level • Linked nodes/asset groups/networks/ hardware • Information for eliminating the vulnerability • Time metrics (dates of detection, opening, last update, eliminating, closing, setting the "false positive" label)	• Number of vulnerable assets • Vulnerability elimination status • Source • Identifiers in different systems • Description • Short description • The way to fix it: • CVSS (Baseline assessment) • CVSS (time assessment) • CVSSv3 (baseline assessment) • CVSSv3 (time assessment) • Exploitability metrics for baseline assessment • Exploitability metrics for baseline assessment • References • Availability of a publicly

					available exploit • Date of the first detection • Date of the last detection • Elimination time • Closing time
Configuring the vulnerability management process	No data available	Setting vulnerability statuses. Manual or automatic assignment of a person responsible for eliminating vulnerabilities and setting deadlines	No data available	Setting vulnerability statuses (open/closed) manually or automatically based on inventory/scan results. Manual or automatic assignment of a person responsible for eliminating vulnerabilities and setting deadlines (depending on the level of criticality). Notification of responsible persons by email. Ability to manually start an incident based on the results of detecting a specific vulnerability, while the incident properties do not dynamically update information about assets with a similar vulnerability discovered later	The vulnerability management process is flexibly configured as part of a logical vulnerability management workflow. There are manual (performing actions at the user's command) and automatic (performing actions when certain conditions occur) transactions-actions on the target system that are configured as part of the inventory workflow using a graphical editor. The actions include creating a new object, changing the properties of the current object, filling guides, executing automation scripts (Bash, PowerShell, Batch, cmd, Java, Javascript, Python), executing queries to external systems, and executing queries to databases. Execution of automation scripts allows launching an arbitrary process of vulnerability processing (installing/removing software, changing registry keys, configuration files, device settings, etc.). The vulnerability management workflow may include setting tasks to eliminate vulnerabilities, routing tasks to performers, monitoring the quality and timing of vulnerability elimination, and so on. There is a chat on objects, in which users of the system can communicate on issues linked to the vulnerability
Virtual patching of vulnerabilities (using the built-in functionality of the	No	No	No	No	Yes, by executing automation scripts

solution)					
2.1.3. Managing tasks, documents, and requirements					
Configuring the task management process	Both manual and automatic task creation are supported	Manual task creation is supported.	Manual task creation is supported.	Both manual and automatic task creation are supported Tasks are automatically created from the "Audit and Control" and "Incidents" modules as a result of linking audit comments to the organization's assets or adding actions on the incident	The task management process is flexibly configured in accordance with the logical workflow, with automatic and manual actions. The task management process can fully reproduce the organization's mechanism for processing requests of any nature, including not only information security / IT tasks, but also arbitrary business processes
Functionality of the task management process	Ability to set the degree of criticality of the task, control execution, send notifications by email. Ability to generate reports on tasks	Viewing tasks in the system interface. Ability to set the degree of criticality of the task, control execution, send notifications by email.	Viewing tasks in the system interface. Ability to set the degree of criticality of the task, control execution, send notifications by email.	Ability to view information on tasks, create a list of tasks, add comments and documents to tasks, export tasks to an Excel file. There is a traffic light indication of the task status, 4 levels of task importance are assigned. Ability to assign a task to the responsible person, email notifications, distribute subtasks to employees with an indication of the parent task (decomposition).	Automatic and manual actions on a task can include notifying users, executing automation scripts on the target system, creating subtasks (decomposition), assigning responsible persons based on task properties, escalating a task when deadlines are exceeded or criticality increases, etc. Maintaining a list of tasks in relation to the role model. The system includes service desk functions with routing and tracking tasks along the L1-L2-L3 lines of SOCs. Ability to manage tasks using the "Knowledge Base/Solutions" functionality, which accumulates and analyzes information on previously solved problems with the ability to find the most suitable solution based on a neural network with dynamic weights and based on the supervised concept. There is a chat on objects, in which users of the system can communicate on assigned tasks
Configuring the document and	Configuring a requirements management process involves	Using the built-in list of standards and	Using the built-in list of standards and	Configuring a requirements management process involves creating	Configuring a requirements management process involves creating

requirements management process	creating a list of standards and regulatory requirements used in auditing.	recommendations, creating personal list	recommendations, creating personal list	a list of standards and regulatory requirements used in auditing. Requirements are linked to a checklist, and custom checklists can be created and weighted. Document management is carried out by creating a list of documents describing protective measures (regulations, policies) with an indication of the approver, the date of creation and planned revision with a reminder of the deadlines. The document is linked the IT infrastructure objects falling under its scope	a list of standards and regulatory requirements used in auditing. Creating a workflow for managing documents and requirements / standards allows implementing arbitrary logic for their processing: assigning responsible persons and deadlines for revision with notification, changing the properties of other objects (for example, increasing the criticality of an asset when it falls within the scope of an industry/ state standard), grouping, exporting/importing, etc.
Functionality of the document and requirements management process	Adding custom standards and regulations is supported.	Adding custom standards and regulations is supported. Creating custom assessments is supported	Adding custom standards and regulations is supported.	Adding custom standards and regulations is supported. Creating control checks, grouped into groups and checklists, to track compliance with requirements and assigned security measures is supported. List of security measures: a custom list, a standard catalog of security measures: R-Vision, SANS CIS Critical Security Controls v6, v7. Loading, changing, deleting any document in the system (including with a file attachment), with automatic assignment of the person responsible for the downloaded object	Adding custom standards, regulations, and regulatory requirements is supported. List of security measures: a custom list, an authoring catalog of security measures: R-Vision, SANS CIS Critical Security Controls v6, v7.
2.1.4. Monitoring the state of information security					
Visualization	Types of graphical display: • Maps • Dashboards Drill-Down functionality	Types of graphical display: • Maps (map modes: world map, link • diagrams) • Charts • Dashboards Drill-Down functionality	Types of graphical display: • Charts • Dashboards	Types of graphical display: • Maps (map modes: world map, network map, room plans, interconnection diagrams) • Charts • Diagrams • Dashboards	Built-in designer of reports and dashboards for using any data and fine-tuning the displayed information. Visualization of arbitrary data obtained by creating SQL queries to the database. Export of graphics as pdf, jpg, png.

				Types of charts: • Audit and control • Incident management (more than 10 preset charts) • Asset management (more than 10 • preset • charts) • Risk management, including visualization of damage from cyber incidents Map functionality: • Displaying incidents, assets, vulnerabilities, and groups of IT assets on geographical maps • Drill-Down functionality (from map to • incidents/assets with detailed view), • Find assets by map • From assets to a network diagram • Displaying assets on floor plans • Export maps (as png) • Import of custom floor plans (png, jpg) Graph functionality: • Specifying a custom time range for plotting • Plotting arbitrary graphs • Plotting graphs based on the parameters of a pre-created filter • Chart constructor (chart types: circular, bar, linear) Diagram functionality: • Linking arbitrary types of incidents/assets with each other	Import of graphics from jpg and png. All graphical views provide object search, Drill-Down, and quick access to linked objects (assets, incidents). Graphical views (widgets) with interaction support for creating dashboards of any composition and configuration. Preset display types for widgets: • Line chart • Histogram (bar chart) • Table • Pie chart • List • Incident calendar Preset visualization displays: • Operational dashboard (information on cyber incidents) • Tactical dashboard (statistical information, visualization of the dynamics of incidents) • General risk dashboard (visualization of the dynamics of cyber risks, risk distribution, history) • Advanced risk dashboard for information systems (risk distribution, history) Geographic map showing buildings, settlements, planets. Displaying features, links, interactions between objects, including assets and incidents; displaying the availability of devices and services. Visualizing of preset objects on the map: • Assets (incidents, vulnerabilities, risks associated with assets)

				• Visualization of assets on a network diagram Dashboard functionality: • Charts and metrics displaying history, current statuses, events and statistics • Visualization of data on equipment, risks, compliance indicators (audit), vulnerabilities, software, OS	• Incidents (with visualization of attack sources and attacked assets) • Branches(display of assets and consolidated information by geographic locations)
Reporting	Export as docx, xlsx, pdf Generation of reports on schedule and manually, sending by email. Generation of custom reports.	Export reports as csv, pdf. Generation of reports on schedule and manually, sending by email. Generation of custom reports.	Export reports Generation of reports on schedule and manually, sending by email. Generation of custom reports.	Export of reports as docx, pdf. Generation of reports on schedule and manually, sending by email. Generation of custom reports. Preset reports. • Cyber risk reporting • Compliance report (GOST R 57580.2-2018, GOST R ISO / IEC 27001-2006, 187-FZ, 152-FZ, NPA the FSTEC of Russia (Orders №№ 17, 21, 31, 239), internal requirements) • Bank reporting (382-P, STO BR, PCI DSS) • Audit report • Report on all types of assets • Vulnerability report • Incident report (summary, statistics, distribution) • Report on the forms of the Central Bank of the Russian Federation (0403202, 0403203) • Threat Model (according to the requirements of the FSTEC of Russia)	Built-in designer of reports and dashboards for using any data and fine-tuning the displayed information. Generation of reports on arbitrary data obtained by creating SQL queries to the database. Full configuration for the needs of the customer. Export of reports as xlsx, docx, pdf, xml, csv. Creation of reports on schedule and manually, delivery by email/to file/via API in xml, pdf, doc, xls, ppt. The ability to generate summary reports/ guides on the parameters of lists, to use analytical and predictive tools for data analysis with function of graphical display, integration with external visualization systems. Automation of internal reporting on existing forms and a report designer for any form: • for different types of audits and separate scans and pen tests • according to the results of the assessment according to the company's methods, the dynamics of changes • to perform the tasks of the department and the task processing flows;

					• according to the auto-SGRC technology; Preset reports. Cyber risk report (summary, detailed) • Compliance report (GOST R ISO / IEC 27001-2006, 187-FZ, 152-FZ, GDPR, NPA the FSTEC of Russia (Orders No. 17, 21, 31, 235, 239), internal requirements) • Bank reporting (GOST R 57580, 382-P, STO BR, PCI DSS, 672-P, 683-P, 684-P, SWIFT CSCF 2020) • Audit report, including the "Auditor's Office" functionality - a dedicated and isolated workspace for external audits • Report on all types of objects, including incidents, assets, and vulnerabilities (dynamics, statistics) Report on the forms of the Central Bank of the Russian Federation (0403202, 0403203) • Threat Model (according to the requirements of the FSTEC of Russia)
Awareness-raising	Internal user knowledge testing system	Training phishing mailings, collecting statistics, training in the system	No data available	Conducting training phishing attacks and training employees in the "Anti-phishing" system	Automated distribution of content: creation / receipt (manually, from external resources), classification and storage, sending by different channels (email, API). Remote questionnaires, feedback forms. Ability to request materials/training-methodological consultations, etc.
Automatic adjustment of tools and systems settings	No	Partially (can be implemented using MS Flow / Power Automate functionality)	No	No	Yes, using the Auto-Compliance tool (authoring auto-SGRC technology): automatic change of OS / software / information security settings to comply with regulatory requirements / return to

					baseline settings
2.2. Cyber risk management					
Configuring the cyber risk management process	Steps for configuring the cyber risk management process: • Manual selection of assets for risk assessment • Assigning a risk owner • Risk assessment: qualitative risk assessment • Partial automatic risk calculation for related assets • Risk treatment: create a risk treatment plan • Reporting	Steps for configuring the cyber risk management process: • Data classification • Connecting data connectors • Selecting and assigning data management policies (DLP setting, Retention Policies, access rights) • Automatic risk assessment • Reporting	Steps for configuring the cyber risk management process: • Defining the business context of risk management • Risk assessment • Configuring risk metrics and controls • Responding to changing risks and control errors	Steps for configuring the cyber risk management process: • Preparation, creation of an assessment: selection of the risk assessment methodology, acceptable risk levels, and asset value assessment. The data is filled in via a questionnaire. Configuring a guide with the degrees of financial, administrative and reputational damage, setting the value of assets • Risk identification: an indication of the sources of threats, prerequisites and implemented protective measures (filled in automatically if the asset is kept under record of security measures). The list of risks is built automatically based on the links in the risk catalogs, while taking into account the links between assets • Risk assessment: it is possible to perform it automatically based on the entered information or manually with experts. Detailed information about risks (sources, prerequisites, protective measures, incidents, treatment plan) is supported • Risk management: create a risk management plan, specify activities (manually or fill in from the risk properties). Types of measures:	Steps for configuring the cyber risk management process: • Defining an organization's risk map • Creating a list of current threats to information security (according to the database of the FSTEC of Russia, a custom list) • Creating a list of vulnerabilities depicting how threats can be implemented (typical vulnerabilities, a custom list) • Creating a list of security measures (standard security measures, a custom list) • Defining the evaluation area and collecting information about current business processes • Creating a threat and intruder model for each asset • Conducting a comprehensive automated assessment of information security risks with the involvement of experts from various structural entities. • Develop a detailed risk management plan, monitor the stages of its implementation and the results of security measures. The task management process is flexibly configured in accordance with the logical workflow, with automatic and manual actions.

				implementation/modification of a protective measure/one-time measure (i.e. risk minimization), risk avoidance, risk transfer. For each event, the responsible person, terms are indicated, and the cost of the event is calculated. It is possible to estimate the cost of implementing the entire risk management plan. • One can view the asset risk management plan from the asset properties and view all planned risk management activities. • Approval of the results of risk assessment • Reporting	• The cyber risk management process can fully reproduce the mechanism for processing risks of any nature adopted in the organization, including building an operating management system (OMS) in accordance with the requirements of the Central Bank of the Russian Federation
Functionality of the cyber risk management process	The following actions are supported for cyber risk management: • Creating a threat model • Risk assessment, incl. derivative risks for related assets	The following actions are supported for cyber risk management: • Automatic generation of a list • of recommendations • Testing recommended actions • Performing recommended actions • Appointment of responsible persons • Monitoring the status of tasks	The following actions are supported for cyber risk management: • Conducting a risk assessment • Preparing and monitoring the implementation of the risk treatment plan • Evaluating the effectiveness of measures taken to handle cyber risks	The following actions are supported for cyber risk management: • Creating a threat model • Risk assessment, incl. derivative risks for related assets • Automatic search for current risks based on threat catalogs (according to the authoring "standard database of threats to information security R-Vision", according to the FSTEC RF DBU, according to the user's catalog of threats) • Preparing and monitoring the implementation of the risk treatment plan • Evaluation of the cost-effectiveness of measures taken to handle cyber risks Risk assessment methods(diagrams): • Custom grading diagram • Authoring R-Vision risk	The following actions are supported for cyber risk management: • Maintaining a register of risks (vulnerabilities, the likelihood of the implementation of threats, assets under threat) • Carrying out a quick risk assessment by company employees • personal business processes without involving employees of the information security department • Visualization of cyber risk information on dashboards • Automatic generation of risk management reports Risk assessment methods(diagrams): • Custom grading diagram • Threat assessment diagram for the project "Methodology for modeling threats to information security" the FSTEC of Russia

				assessment diagram • Simplified qualitative assessment diagrams • Simplified quantitative assessment diagrams • Threat assessment diagram for the project "Methodology for modeling threats to information security" the FSTEC of Russia • According to the risk assessment methodology of the Central Bank of the Russian Federation (RS BR IBBS-2.2-2009) • According to international methodologies (ALE, FAIR, ISO 27005, NIST, OCTAVE) Preset guides: • threat modeling • intruder simulation • conducting a risk assessment Creating custom guides is not supported, but it is possible to add new items to existing ones. The creation of custom criteria for evaluating the value of assets is supported. Link between the risk assessment of an asset and incidents that have occurred with it is supported. Creating user-defined threats limited to threat types in accordance with the 1119-RGRF methodology in terms of the relevance of threats to the use of UDF in system / application software. Logging of all completed actions when working with cyber risks is supported.	• According to the risk assessment methodology of the Central Bank of the Russian Federation (RS BR IBBS-2.2-2009) • According to international methodologies (FAIR, OCTAVE, ALE, ISO 27005, NIST, Quantitative Risk Assessment Method) There are manual (performing actions at the user's command) and automatic (performing actions when certain conditions occur) transactions-actions on the target system that are configured as part of the cyber risk management workflow using a graphical editor. As actions, it is envisaged to create a new object (including, for example, an application for filling out a risk questionnaire by an expert), notifying responsible employees (for example, risk owners), executing automation scripts (Bash, PowerShell, Batch, cmd, Java, Javascript, Python), execution of queries to external systems, execution of queries to databases. Execution of automation scripts allows starting the flow of processing cyber risks (changing device settings and SPI/software/OS, installing / removing software, returning assets to their baseline state). The workflow of cyber risk management may include setting tasks for the implementation of the risk management plan items, routing tasks to performers, monitoring the quality and timing of the measures taken to process risks, etc. There is a chat on objects, within

					which users of the system can communicate on tasks related to a specific risk/threat/ vulnerability/security measure. Logging of all completed actions as part of the cyber risk management workflow is supported
2.3. Audit and compliance management					
Configuring the audit and compliance management process	No data available	Steps for configuring an audit and compliance management process: • Selecting relevant standards • Refinement of the list of requirements for a specific infrastructure • Selection of security measures (controls) • Conducting a compliance assessment • Assigning tasks, responsible people • Reporting, monitoring of implementation	No data available	Steps for configuring an audit and compliance management process: • Uploading a list of audit requirements/standards to the system • Setting up the scale of assessments, levels of audit comments, as well as a set of checks related to the requirements of the applicable standards • Scheduling audits to support this action from asset properties. The asset is linked to a list of implemented protective measures and applicable requirements • Conducting an audit with support for sending an email notification about the date of the audit, collaboration (assigning grades and comments on the audit, chatting on the audit), the ability to attach an attachment to the audit task, creating reports • Making and analyzing audit comments with the selection of comments from the drop-down list or filling in manually • Preparing and monitoring the implementation of plans to eliminate comments, creating an appropriate task,	With the help of the auto-Compliance tool (authoring auto-SGRC technology), the audit and compliance management process can be flexibly configured in accordance with a logical workflow. Steps for configuring an audit and compliance management process: • Creating a list of requirements • Configuring the audit and compliance management workflow • Collecting information and statistics • Creating control objects • Preparing checklists • Assessing the fulfillment of requirements • Reporting • Preparation of the "Auditor's Office" - a dedicated and isolated workspace for external audits • Adjusting the settings of devices, software, information security systems, OS for automatic elimination of identified comments

				decomposing activities and tasks into subtasks	
Audit and compliance management process functionality	The following actions are supported to manage audits and compliance: • Creating models of violators and threat models according to the requirements of the FSTEC and the FSB • Preparing documentation for compliance with the legislation on personal data protection • Designing an audit program, forming a plan and an audit team • Creating custom evaluation criteria with weights • Generating reports and a list of comments • Ability to attach audit certificates	The following actions are supported to manage audits and compliance: • Selecting requirements for a specific industry (finance, energy, education, medicine, government organizations) • Selecting applicable legal requirements, including GDPR, HIPAA, SOX, SoX, etc. • Planning activities for compliance with GDP, ISO 27001, NIST 800-53 • Creating personal requirements • Notifying responsible people for tasks by email • Performing actions using the MS Flow / Power Automate constructor with the ability to partially automate the actions performed.	The following actions are supported to manage audits and compliance: • Selecting Requirements (Use Case) for a specific industry • Selecting applicable requirements • Creating personal requirements • Notifying responsible people for tasks	The following actions are supported to manage audits and compliance: • Preparing and controlling audit comments with automatic creation of the corresponding task for the responsible employee to eliminate shortcomings, with synchronization of the task and comment statuses, with notification of responsible persons by email, with support for sending tasks for eliminating comments to external Service Desk systems Conducting control checks - monitoring compliance with legal regulations and security measures. Assigning audit checks to assets after linking the assets to security measures and sets of requirements. Setting the frequency of control checks, appointing responsible employees, auditors. Manual generation of a list of requirements for control checks. Manual assessment of compliance with the requirements of the control check: appointment of responsible experts, combining them into working groups, conducting an expert assessment with justification, issuing an audit assessment based on the control checks carried out • Calculating the quantitative index of compliance with the requirements based on expert assessments, taking into	The following actions are supported to manage audits and compliance: • Centralized management of the audit process, ensuring that data is always up-to-date • Execution of automation scripts allows starting the flow of eliminating the comments identified during the audit (changing the settings of devices and ISS / software / OS, installing / removing software, returning assets to their baseline state) • the audit and compliance management workflow may include setting tasks for the implementation of the audit plan items, routing tasks to performers, quality control and deadlines. • measures taken to eliminate the comments identified during the audit, etc. • Launching audit and related activities as part of a single process • Creating and automatically tracking audit schedules • Ability to create personal audit methods (according to the company's methods) • GAP analysis (comparison of the current and target state • There is a chat on objects, in which users of the system can communicate on issues related to audit and compliance with requirements • Logging all completed actions as part of the audit and compliance management

				account the weights of the requirements. Ability to add custom evaluation methods using the audit type constructor using formulas, tables, and lists • Visualizing the performed control checks: output of tables with a list of audit grades, graphic diagrams (dashboards) The involvement of different experts at different stages of audit and compliance management is supported. Viewing audit results and elimination work plans directly from asset properties is supported Support for performing simple (one asset - one questionnaire) and summary (multiple questionnaires for multiple assets, verification by different standards) audits. Comprehensive audit support: aggregating multiple audits into a single final compliance assessment. Automatic dynamic recalculation of audit indicators when the verification method is changed, automatic execution of scheduled checks, automatic notifications to users. Import / export of assessment results as Excel. Import of audit requirements from csv, xlsx. Preset standards for conformity assessment: 152-FZ, NPA the FSTEC of Russia (Orders Nos. 17, 21, 31, 239), PCI DSS (3.1, 3.2), SWIFT's Customer Security Program, ISO 27001, GOST R ISO / IEC 27001-2006 , 382-P, STO BR IBBS-1.0-2014,	workflow is supported Automation modules: • audit reports • accounting for external flows of personal data of the organization, subsidiaries and affiliates and companies of the ecosystem • monitoring the processing and protection of data in the companies of the ecosystem and partners of the organization • accounting and monitoring the results of control processing and data protection in the companies of the ecosystem and partners of the organization • expert examinations in relation to pilot processes, accounting for materials and results of the expert examination • preparing checklists • preparing reports in terms of external control and expertise End-to-end compliance of checks in different company standards and regulations, without the need to repeat checks for each standard. Availability of metrics and analysis of conducted audits. Ability to import into the system the results of previously made audits in order to work with them Role model for generation and approval of the audit report. Maintaining a plan for eliminating

				GOST R 57580.2-2018	audit comments, with automatic tracking and notification. Remote questioning with a separate verification function is supported, the ability to attach file and other audit evidence. Visualizing audit schedule execution: • progress on the number of identified comments • speed of elimination of comments • prompt preparation and implementation of a plan to eliminate comments • comment statistics Export of assessment results as xlsx, docx, pdf. Import of audit requirements from csv, xlsx. Yes, preset regulations: 187-FZ, 152-FZ, GDPR, the FSTEC of Russia (Orders No. 17, 21, 31, 235, 239), PCI DSS (3.1, 3.2), SWIFT's Customer Security Program, SWIFT CSCF 2020 , ISO 27001, GOST R ISO / IEC 27001-2006, 382-P, 672-P, 683-P, 684-P, 716-P, STO BR IBBS-1.0-2014, GOST R 57580.2-2018
Automatic compliance with standards	No	No	No	No	Yes, using the Auto-Compliance tool (authoring auto-SGRC technology): automatic change of OS / software / information security settings to comply with regulatory requirements. Automating compliance with requirements: • GOST R 57580.1 • 382-P • PCI DSS • 187-FZ • GDPR • ISO 2700X • and etc. Any proprietary enterprise standard is

					automated.
CII security support	No data available	No	No	System capabilities to support CII security: • Accounting for CII subjects • Collecting characteristics of CII subjects • Assessment of the criticality of the processes of the CII subject • Collecting data on the composition of the object CII (CIIO) • Inventory of equipment and software in CIIO with entry into the CIIO card • Preparing the list of CIIO , modeling of threats to CIIO according to the methodology of the FSTEC of Russia • Calculation of the relevance category for CIIO • Accounting for CII security measures • Conducting an audit for compliance with the Order of the FSTEC of Russia No. 239 for CIIO (CIIP) • Preparing documents for submission to the FSTEC of Russia	System capabilities to support CII security: • Aggregation of information: about the subject of CII, about the person operating CII, about CII, about the interaction of CII and telecommunication networks, about the software and software and hardware used at CII • Preparing information about threats to the security of information and categories of offenders in relation to CIIO (with the participation of experts) • Preparing possible consequences in the event of computer incidents (with the participation of experts) • Assigning categories • the relevance of CIIO (with the participation of experts) • Preparing organizational and technical measures used to ensure the CIIP security (with the results being uploaded as pdf and docx) • The relevance category revision process is supported • Preparing a list of control measures (checklist) of the basic set of CIIP measures based on the assigned category and adaptation of the set of basic measures in accordance with the CIIP threats and characteristics (downloading as docx) • Creating and controlling the execution of tasks for the implementation of missing measures • Decommissioning procedure of the OCII (formation of a set of documents) is supported

Conclusions on Section No. 2

In terms of information security management, as in the previous section, the most attractive solutions are the American Microsoft Compliance Center as well as the domestic R-Vision and Security Vision. They are leading in terms of the amount of collected and inventory information about equipment, the ability to integrate with third-party solutions, and vulnerability management (note that in terms of the types of vulnerabilities processed, Microsoft Compliance Center and Security Vision are leading - they handle both software vulnerabilities and configuration vulnerabilities, while ePlat4m, RSA and R-Vision only handle software vulnerabilities). In terms of managing tasks, documents, and requirements, along with Microsoft Compliance Center, R-Vision, and Security Vision, ePlat4m also demonstrates some good features. In terms of monitoring the state of information security, Microsoft Compliance Center, R-Vision and Security Vision are also the most attractive. At the same time, Security Vision provides the most extensive information visualization and reporting capabilities.

In the management of cyber risks and compliance with legal requirements, ePlat4m and RSA demonstrate rather modest functionality. The RSA system is also quite closed and is focused more on the Western consumer, or on the Russian subsidiary of such a company.

The functionality of the Microsoft solution is much more advanced in this regard. Automation using MS Flow / Power Automate is especially noteworthy, which allows flexibly managing IT and information security processes, as well as solving a large number of business problems.

The R-Vision cyber risk management functionality is distinguished by the fact that, in our opinion, the product was originally "tuned" for banks; there is also a wide set of preset bank reports. This solution is likely to be well suited for financial organizations that implement standard banking business processes and that will have enough preset options for working with risks, compliance and reporting. Among the disadvantages of the R-Vision solution, we can distinguish weak configuration options for the needs of specific organizations. Many functionalities and even non-critical parameters are “hard-wired” in the system and cannot be configured and changed by the end user: for example, asset and vulnerability management processes are straightforward enough, without support for branching processes, and risk and compliance management processes are not suitable for large companies with extensive structure and complex processes.

Security Vision is flexible in configuration, which allows the end user of the system not only to change the parameters of the existing information security management processes, but also to create their own processes that will most closely match those adopted in the organization. However, it should be taken into account that for a high-quality configuration of this solution, one will need to allocate significant time resources, and it is also desirable to have a specialist who supports this system (fortunately, the vendor conducts training for the customers and partners). Among the most notable innovations of Security Vision: 1. An incident analysis module containing a machine learning model and the ability to automatically determine incident response commands and transmit incident response commands to connected external systems and devices is the embodiment of the practical use of Artificial Intelligence in solving applied IS problems. 2. The auto-SGRC functionality (authoring technology), which allows real-time compliance with the requirements of regulators and proprietary standards, automatically adjusting OS, software and information security settings, has no analogues in the domestic market.

General conclusions

The review involved SGRC products, which are quite different both in ideology and architecture, and in functionality.

ePlat4m is actually a "boxed" solution without flexible and precise configuration, however, according to a number of parameters, it seems promising and has actual basic parameters.

Microsoft's solution should be commended. In terms of functionality, we would especially like to note automation using MS Flow / Power Automate, which allows flexible management of IT and information security processes, as well as solving a large number of business tasks. The disadvantage of this solution for domestic customers may be the fact that Microsoft Compliance Center operates in the Azure cloud infrastructure and it is optimized for this ecosystem, so it will not be possible to use it separately. The RSA Archer solution, being not cloud-based, is also focused on application in the RSA product stack. The main disadvantage of solutions from Microsoft and RSA is the potential complexity of their purchase and implementation in many domestic companies bound by strict legal regulations.

The R-Vision solution has developed functionality and, in our opinion, is focused on banks, and with quite typical business processes: deep customization and configuration of various parts of the solution by the user is not provided. However, this product gives the impression of a solid "monolith" that, once configured, will be able to meet the requirements of a number of financial organizations.

The Security Vision solution looks to be the most flexible of all the reviewed products and, in our opinion, is able to reproduce rather complex business processes and adapt to the needs of a customer from any industry. Security Vision offers the largest variety of connector types and capabilities. However, of course, this involves a long-term configuration and optimization of the product for the individual characteristics of each specific organization. The auto-SGRC functionality used by Security Vision to automate regulatory compliance with changes in the settings of the monitored infrastructure looks a significant advantage.

A notable difference between the Russian systems, i.e., ePlat4m, R-Vision, and Security Vision, is their inclusion in the Russia's Unified Register of Russian Programs for Electronic Computers and Databases. In addition, R-Vision and Security Vision have certificates of compliance with the FSTEC of Russia.