**Technical requirements**

**for the development**

**Software product «Information exchange module»**

**and**

**Software product «Information collection module»**

**Kyiv 2025**

Content

[Abbreviations and terminology 4](#_Toc208311044)

[1 General information about the content of the works 6](#_Toc208311045)

[1.1 Full name of the informatization object 6](#_Toc208311046)

[1.2 Beneficiary information 6](#_Toc208311047)

[1.3 List of regulatory documents that should be taken into account during development 6](#_Toc208311048)

[2 Purpose and goals of informatization 8](#_Toc208311049)

[2.1 Purpose 8](#_Toc208311050)

[2.2 Goals of informatization 8](#_Toc208311051)

[3 Description of the informatization object 10](#_Toc208311052)

[4 Requirements for the informatization tool 13](#_Toc208311053)

[4.1 Requirements for the structure and functioning of the informatization tool 13](#_Toc208311054)

[4.2 Requirements for the number and qualifications of the staff of the informatization tool and its mode of operation 15](#_Toc208311055)

[4.3 Requirements for security 16](#_Toc208311056)

[4.3.1 Requirements for segregation and access control 16](#_Toc208311057)

[4.3.2 Requirements for authentication and authorization 16](#_Toc208311058)

[4.3.3 Requirements for data encryption and protection 17](#_Toc208311059)

[4.3.4 Requirements for logging and auditing 18](#_Toc208311060)

[4.3.5 Compatibility with antivirus protection and limits of liability 18](#_Toc208311061)

[4.3.6 Other security requirements 18](#_Toc208311062)

[4.4 Requirements for ergonomics and technical aesthetics 20](#_Toc208311063)

[4.5 Information protection requirements 20](#_Toc208311064)

[4.6 Requirements for standardization and unification 21](#_Toc208311065)

[4.7 Requirements for the reliability of the informatization tool and the preservation of information 22](#_Toc208311066)

[4.7.1 General requirements for reliability 22](#_Toc208311067)

[4.7.2 Reliability criteria 23](#_Toc208311068)

[4.7.3 Disaster recovery 24](#_Toc208311069)

[4.7.4 Backup and recovery capabilities requirements 24](#_Toc208311070)

[4.8 Requirements for methods and means of communication for information exchange between the components of the informatization tool 24](#_Toc208311071)

[4.9 Requirements for operating modes and productivity of an informatization tool 24](#_Toc208311072)

[4.10 Requirements for functions (tasks) performed by an informatization tool 25](#_Toc208311073)

[4.10.1 Approximate principle scheme of the proposed solution 25](#_Toc208311074)

[4.10.2 General requirements for the functionality of SWPs 31](#_Toc208311075)

[4.10.3 General requirements for the Software product "Information exchange module" 32](#_Toc208311076)

[4.10.4 Functional requirements for the Software product "Information exchange module" 35](#_Toc208311077)

[4.10.5 General requirements for the Software product "Information collection module" 43](#_Toc208311078)

[4.10.6 Functional requirements for the Software product "Information collection module" 44](#_Toc208311079)

[5 Requirements for development and transfer of services 53](#_Toc208311080)

[5.1 Requirements for the development 53](#_Toc208311081)

[5.2 Requirements for the transfer of services 53](#_Toc208311082)

[5.2.1 Requirements for the order of deployment 53](#_Toc208311083)

[5.2.2 Requirements for functional testing 54](#_Toc208311084)

[5.2.3 Requirements for penetration testing of SWPs 54](#_Toc208311085)

[5.2.4 Acceptance procedure 54](#_Toc208311086)

[5.2.5 Requirements for support by the Supplier 55](#_Toc208311087)

[5.2.6 Requirements for personnel training 55](#_Toc208311088)

[5.3 Requirements for warranty support 55](#_Toc208311089)

[6 Conclusions 58](#_Toc208311090)

[7 Annexes 59](#_Toc208311091)

[7.1 Annex 1. Layout of the information card for the subject of the inspection 59](#_Toc208311092)

[7.2 Annex 2. List of external sources of information 60](#_Toc208311093)

[7.3 Annex 3. Stage implementation schedule 61](#_Toc208311094)

[7.4 Annex 4. Requirements for potential suppliers 62](#_Toc208311095)

# Abbreviations and terminology

|  |  |
| --- | --- |
| Abbreviation | Definition |
| API | Application Programming Interface |
| Beneficiary | For the Software product «Information exchange module»:  • State Judicial Administration.  For the Software product «Information collection module»:  • High Qualification Commission of Judges in Ukraine. |
| CIPS | Comprehensive information protection system |
| CIPT | Cryptographic information protection tool |
| DBMS | Database management system |
| ESoI | External sources of information |
| HQCJ | High Qualification Commission of Judges in Ukraine |
| Interface | A set of rules and protocols that ensure interaction between a user and a computer or between different software components |
| IS | Information system |
| (the) Law | Law of Ukraine "On the Judicial System and the Status of Judges" |
| Logging | The process of recording information about events that occur in the operating system, programs, or networks |
| NACP | National Agency on Corruption Prevention |
| OS | Operating system; software that manages the hardware resources of a computer or server and ensures the execution of programs. It is the basis for the operation of other programs and provides an interface between the user and the computer hardware |
| Other UJICS modules | Other specialized UJICS software modules that implement the initialization of requests through the Software product "Information exchange module" to external information sources and the analysis of the responses received from them |
| QES | Qualified electronic signature |
| QETSP | Qualified electronic trust service provider |
| SAPR (HQCJ) | Workflow automation system of the High Qualification Commission of Judges in Ukraine |
| SE ICS | State Enterprise "Information Court Systems" |
| SJA | State Judicial Administration |
| Software product | Software, the result of computer programming in the form of an operating system, system, application, entertainment and/or educational computer program (their components), as well as in the form of Internet sites and/or online services and access to them, copies (instances) of computer programs, their parts, components in material and/or electronic form, including in the form of code (codes) and/or links for downloading a computer program and/or their parts, components in the form of code (codes) for activating a computer program or in another form, cryptographic means of information protection |
| Software product «Information collection module» | Software product that implements the collection and processing of information received from ESoI to verify information regarding the compliance of a judge (candidate for the position of a judge) with the rules of professional ethics and the compliance of the judge (candidate for the position of a judge) with the criterion of integrity, including the compliance of the expenses and property status of the judge (candidate for the position of a judge) and his family members. |
| Software product «Information exchange module» | Software product that implements electronic information interaction with external information sources (registers, databases, etc.) |
| Sources of information | Electronic register - an information and communication system that ensures the collection, accumulation, protection, accounting, display, processing of register data and the provision of register information |
| Supplier | A legal entity that will be selected through an open competition to develop and implement SWPs. |
| SW | Software; a set of instructions, data, or programs used to control computer hardware and perform specific tasks. It includes operating systems, application programs, and utilities that enable the computer system to function and interact with the user. |
| SWPs | Software product «Information collection module» and Software product «Information exchange module» |
| Transaction | A completed logical block of operations in an information system, the execution of which ensures the integrity and consistency of data. Each transaction has a unique number for identification and registration in the event of an error or incorrect processing. |
| Trembita | System of electronic interaction of state electronic information resources (Ministry of Digital Transformation of Ukraine) |
| UJICS | Unified judicial information and communication system or Unified judicial information and telecommunications system (until the name is unified in regulatory legal acts) |

# General information about the content of the works

## Full name of the informatization object

Full name of the informatization object:

* Software product «Information exchange module»;
* Software product «Information collection module».

(hereinafter collectively – SWPs).

## Beneficiary information

Beneficiary information for Software product «Information exchange module»:

* State Judicial Administration (hereinafter – SJA).

Beneficiary information for Software product «Information collection module»:

* High Qualification Commission of Judges in Ukraine (hereinafter – HQCJ).

## List of regulatory documents that should be taken into account during development

When designing and creating SWPs, the requirements of such applicable regulatory documents must be taken into account:

* Law of Ukraine “On the Judiciary and the Status of Judges” (hereinafter – the Law);
* Law of Ukraine “On Electronic Identification and Electronic Trust Services”;
* Law of Ukraine “On Prevention of Corruption”;
* Law of Ukraine “On Protection of Information in Information and Communication Systems”;
* Law of Ukraine “On Protection of Personal Data”;
* Law of Ukraine “On Information”;
* Law of Ukraine “On Public Electronic Registries”;
* Law of Ukraine “On Access to Public Information”;
* Law of Ukraine “On Basic Principles of Ensuring Cybersecurity of Ukraine”;
* Decree of the President of Ukraine dated 27.09.1999 No. 1229 “On Approval of the Regulations on Technical Protection of Information in Ukraine” (as amended);
* Resolution of the Cabinet of Ministers of Ukraine dated February 21, 2025 No. 205 “Some Issues of Creation, Administration and Ensuring the Functioning of an Information Means” (as amended);
* Resolution of the Cabinet of Ministers of Ukraine dated 26.03.2006 No. 373 “On Approval of the Rules for Ensuring Information Protection in Information, Communication and Information and Communication Systems” (as amended);
* Resolution of the Cabinet of Ministers of Ukraine dated 27 January 2010 No. 55 “On Streamlining the Transliteration of the Ukrainian Alphabet into the Latin Alphabet” (as amended);
* DSTU ISO/IEC/IEEE 12207:2018 “Systems and Software Engineering. Software Lifecycle Processes”;
* DSTU ISO/IEC 40500:2015 “Information Technologies. Web Content Accessibility Guidelines W3C (WCAG) 2.0”;
* DSTU ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection. Information security management systems. Requirements.;
* Decision of the High Council of Justice of January 17, 2019 No. 141/0/15-19 “On approval of the Regulations on the State Judicial Administration of Ukraine” (as amended).

# Purpose and goals of informatization

## Purpose

SWPs are designed to automate the process of entering, transmitting, processing, presenting information and accessing it about judges and candidates for the position of judge, including their family members and close relatives (Part 1, Article 86 of the Law of Ukraine "On the Judiciary and the Status of Judges"), from open and specialized registers and information systems.

SWPs provide:

* initiating requests to authorized state bodies and electronic registers;
* receiving responses to requests and the results of their processing;
* automated processing of received data;
* generating a unified report (information card on the subject of the inspection; provided in Annex 1).

SWPs are focused on the use of SJA and HQCJ within the powers defined by the Law of Ukraine “On the Judiciary and the Status of Judges” and the Law of Ukraine “On Prevention of Corruption”, to select candidates for appointment to the position of judge, conduct qualification assessments, maintain a judicial dossier and a dossier of a candidate for the position of judge, as well as exercise other powers defined by the Law.

## Goals of informatization

The main goals of informatization are:

1. Increasing the efficiency of the inspection of judges and candidates for the position of judge by automating the processes of collecting and analyzing data from external sources.
2. Ensuring the transparency of the inspection procedures specified by the Law.
3. Ensuring the reliability of information used in the procedures specified by the Law for the selection of judges, appointment and transfer to the position of judge, and qualification assessment of judges.
4. Reducing the administrative burden on HQCJ employees by automating repetitive operations.
5. Improving the quality and completeness of the assessment of judges and candidates for the position of judge by using a wide range of data sources, including real estate registers, vehicles, declarations, data on family ties, etc.
6. The possibility of integration with other external sources of information (hereinafter – ESoI), in particular through “Trembita”, to ensure the relevance and efficiency of the information received.
7. Creation of a single unified report with the ability to view, analyze, save and export the received information in a structured form.
8. Ensuring the lawful and secure processing of personal data in accordance with the requirements of the law.
9. Ensuring relevance: the information received, processed and stored in the judicial dossier must meet the purposes of its collection and not be excessive for the implementation of the purpose of maintaining the judicial dossier.

# Description of the informatization object

The SJA is a state body in the justice system that provides organizational and financial support for the activities of judicial authorities within the powers established by law, in order to create appropriate conditions for the functioning of courts and the activities of judges (paragraph 1 of the Regulation on the State Judicial Administration of Ukraine).

One of the main tasks of the SJA is to ensure appropriate conditions for the activities of courts, the High Qualification Commission of Judges of Ukraine, the National School of Judges of Ukraine and judicial self-government bodies within the powers established by law (paragraph 2 of the Regulation on the State Judicial Administration of Ukraine).

In accordance with the specified tasks, the SJA, among other things, ensures the implementation of an electronic court, takes measures to organize the exchange of electronic documents between courts and other state bodies and institutions (subparagraph 12 of paragraph 5 of the Regulation on the State Judicial Administration of Ukraine).

HQCJ shall verify information regarding a person applying for a position involving a responsible or especially responsible position and positions with an increased corruption risk in accordance with Article 793 of the Law.

In accordance with Article 75 of the Law, after adopting a decision on admitting candidates for the position of a judge to a special inspection, HQCJ shall send requests to authorized state bodies for information regarding the candidates regarding their compliance with the requirements specified by the Law and the authenticity of the documents submitted by the person.

The list of authorized state bodies, the terms and requirements for information to be provided or received shall be determined by HQCJ taking into account the information contained in the dossier of candidates for the position of a judge or the judicial dossier.

In the event that the HQCJ receives information through electronic interaction with automated information and reference systems, registers and data banks, the holders (administrators) of which are state authorities, other state authorities or local self-government bodies, written requests to the relevant bodies are not sent.

In order to form a judicial dossier (filing of a candidate for the position of a judge), conduct a special check, verify reports of inaccuracy of statements in declarations of integrity and family ties, the HQCJ also has the right to receive information free of charge regarding the judge (candidate for the position of a judge) and his family members or close persons in the manner provided for in Article 86 of the Law, including the HQCJ has the right to receive information and copies of documents and materials (including those with limited access) regarding the judge (candidate for the position of a judge) and his family members or close persons free of charge from any persons who are the owners or managers of the information (documents, materials) requested.

According to Article 85 of the Law, the judicial dossier must contain information on the judge’s compliance with the rules of professional ethics and the judge’s compliance with the criterion of integrity, including the compliance of the expenses and property of the judge and his family members, as well as close persons with the declared income, including copies of the relevant declarations submitted by the judge in accordance with the legislation on the prevention of corruption.

According to Clause 3 of Part Five of Article 85 of the Law, the dossier of a candidate for the position of a judge must contain materials from a special inspection and other information on the candidate for the position of a judge’s compliance with the criterion of integrity, in particular, the compliance of the expenses and property of the candidate for the position of a judge and his family members with the declared income, including copies of the declarations submitted in accordance with this Law and the legislation on the prevention of corruption.

According to Article 60 of the Law, a full verification of the declaration of a person authorized to perform state or local government functions, submitted by a judge, is carried out by the NACP, and consists in clarifying the reliability of the declared information, the accuracy of the assessment of the declared assets, checking for the presence of a conflict of interest and signs of illicit enrichment.

In order to prepare for a special verification of a candidate for the position of judge, in accordance with Article 793 of the Law, Articles 56–58 of the Law of Ukraine “On Prevention of Corruption”, the HQCJ may receive the following information from the NACP:

* information on the availability of information about the candidate in the Unified state register of persons who committed corruption or corruption-related offenses;
* information on the reliability of the information specified by the candidate in the declaration of a person authorized to perform state or local government functions for the past year;
* information that may indicate the candidate's compliance or non-compliance with the criteria of professional ethics, competence or integrity (if any).

The combined information from the person’s declaration and the results of the NACP verification of the information indicated by the declarant in the declaration, including information on the property of his family members, is for the HQCJ a reliable source of information on the property status of the judge (candidate) and his family members and the compliance of expenses. However, the information received from the NACP on the property status of the person relates exclusively to the result of the verification of the person’s declaration, in which the person indicates his family members in accordance with Art. 1 of the Law “On Prevention of Corruption”, notes to Art. 46 of the Law “On Prevention of Corruption”, namely:

* persons who are married to the reporting entity (husband/wife) as of the last day of the reporting period, regardless of cohabitation with the reporting entity during the reporting period;
* children of the reporting entity until they reach the age of majority, regardless of their cohabitation with the reporting entity during the reporting period;
* any persons who, as of the last day of the reporting period (provided that they cohabited with the reporting entity during the 30 calendar days preceding the last day of the reporting period) or for a total of at least 183 days during the year preceding the year of filing the declaration:
  + lived together;
  + were connected by a common life;
  + had mutual rights and obligations with the subject of the declaration (except for persons whose mutual rights and obligations are not of a family nature), including persons who lived together with the subject of the declaration, but were not married.

All other persons, in the absence of at least one of the above-mentioned characteristics, are not considered family members of the subject of declaration for the purposes of declaration.

HQCJ to verify information on the judge's compliance with the rules of professional ethics and the judge's compliance with the criterion of integrity, including the compliance of the expenses and property of the judge and his family members, uses another principle of forming a connection, for example, Article 61 of the Law for filling out the declaration of family ties of a judge to persons with whom the judge is related, including:

* persons who live together, are connected by a common life and have mutual rights and obligations with the judge (except for persons whose mutual rights and obligations with the judge are not of a family nature), including persons who live together but are not married to the judge;
* regardless of the conditions specified in paragraph 1 - husband, wife, as well as relatives of each spouse or relatives of persons who live together but are not married to the judge (father, mother, stepfather, stepmother, son, daughter, stepson, stepdaughter, brother, sister, grandfather, grandmother, great-grandfather, great-grandmother, grandson, granddaughter, great-grandson, great-granddaughter, son-in-law, daughter-in-law, father-in-law, mother-in-law, nephew, niece, uncle, aunt, cousin, adopter, adopted).

Thus, HQCJ requires a decision on the creation of a system for collecting and analyzing information to verify information on compliance by candidates for judicial positions, judges with the rules of professional ethics and compliance of judges with the criterion of integrity, including compliance of expenses with the property of judges and family members and close persons.

The technical administrator of SWPs will be the State Enterprise "Information Court Systems" (hereinafter - SE ISC) - a state commercial enterprise, which is based on state ownership and belongs to the sphere of management of the SJA (the charter of the enterprise was approved by the SJA order of 26.11.2019 No. 1142).

# Requirements for the informatization tool

## Requirements for the structure and functioning of the informatization tool

The decision to build SWPs should be based on the following principles:

* use of modern information technologies;
* implementation of the concept of a single information space within the Unified judicial information and communication system (hereinafter – UJICS), as well as integration with external information systems;
* adherence to the principle of centralized information exchange;
* maintaining the relevance, completeness, consistency, integrity and availability of data;
* reliable protection of information from integrity violations, unauthorized access, leakage and blocking, including using encryption and hashing mechanisms, in accordance with the requirements of regulatory legal acts in the field of information security;
* high reliability and redundancy of technical infrastructure components;
* centralized management, constant monitoring of the performance and centralized configuration of software and its components;
* application of modern software engineering methods during the development of application software.

The SW architecture should provide for maximum independence of software and technical components from the developer in such a way that their further development can be carried out by the technical administrator of the SWPs and / or contracting organizations with the appropriate level of qualification.

Each SWPs should have the following characteristics and functionality:

* have a single central database of information for temporary storage of transit information. The storage period must be additionally agreed upon by the Supplier and the Beneficiary at the stage of “Development of the technical specification”;
* support the use of an open-source database management system (hereinafter – DBMS);
* provide the necessary means of automated data integrity control and consistency of stored information, personalization of data created by different users, and keeping a log of operations performed;
* provide mechanisms for administering users and their authorizations, as well as ensuring the protection of personal data in accordance with the current legislation of Ukraine;
* be sure to document APIs in accordance with international types of specifications and ecosystems, such as: Swagger, RAML, API Blueprint or analogues for use by internal/third-party services. Preference is given to the tool that provides the best support at the time of component development in terms of libraries, frameworks aimed at use in different programming languages, their maturity;
* use of information exchange formats based on the following protocols and standards: HTTPS, JSON, REST (Restfull).

WEB components of SWPs must be accessible from automated user workstations without the need to install client software components of SWPs on them (this requirement may not apply to cryptographic libraries for qualified electronic signatures).

All third-party software components licensed separately and planned for use in SWPs, the cost of their licenses and technical support must be submitted as part of the offer, including the Supplier must provide a separate calculation of the cost of ownership for 10 years. The Supplier must provide information about all third-party components of application SW and DBMS planned for use in SWPs (this requirement may not apply to cryptographic libraries for qualified electronic signatures). The specified SW is also subject to warranty service requirements. The Beneficiary reserves the right to obtain licenses for SW from third-party developers according to a separate procedure.

For their work, SWPs may rely on software products and solutions and use databases that are distributed as free SW (note: FLOSS — free/libre/open source software — software distributed under so-called free or open license agreements).

Any open source software products (libraries, dependencies or parts of the program code) that will be used in the components of SWPs must be approved by the Beneficiary. Requirements for warranty support, including for third-party software solutions, are specified in section 5.3 “Requirements for warranty support”.

SWPs must provide for horizontal scaling according to the principles of microservice architecture.

SWPs should be built on a client-server architecture and should have a three-tier architecture, i.e. the user interface layer (browser), application layer (application server) and data layer (database) should be distinguished in the SWPs architecture.

SW SWPs should support the development of SWPs' capabilities for connecting additional equipment, i.e. the performance of SWPs will be easily increased by adding additional technical resources without modifying the SW source code.

Connecting additional equipment (adding additional technical resources) to increase SWPs' performance should not require modifying the SW source code.

The client part of SWPs should meet the following requirements:

* on user workstations, all functionality of the client part of SWPs (full-featured web client) must be available using an Internet browser as a web client (Google Chrome, Mozilla FireFox, Opera or another browser that will meet the security and reliability requirements for the operation of these SWPs) and operate under the control of OS Windows or OS Linux/Unix as the most widely used;
* on client workstations, it may be required to install an Internet browser, as well as SW responsible for the operation of SWPs with a qualified electronic signature and peripheral devices that ensure data security.

SWPs must be designed for operation as part of the Beneficiary software and hardware complex. Technical and physical protection of SWPs hardware components, data carriers, uninterrupted power supply, resource backup, and ongoing maintenance are implemented by the Beneficiary using technical and organizational means provided for in the Beneficiary IT infrastructure.

The possibility of performing routine maintenance work on SWPs with a guarantee of preservation and automatic recovery of unprocessed tasks that were in processing queues on the server side must be ensured. The list of routine work, their frequency, responsible persons, and the procedure for recording results must be approved in the relevant administrative document of the Beneficiary at the stage after experimental operation of SWPs.

## Requirements for the number and qualifications of the staff of the informatization tool and its mode of operation

The State Enterprise "Information Court Systems" (hereinafter - SE ICS) will be appointed as the technical administrator of the information technology facility being created, which was created to provide services for technical and technological support for the creation and maintenance of software for maintaining automated systems (electronic databases), in particular, state registers created in accordance with the laws of Ukraine, regulatory legal acts of the Cabinet of Ministers of Ukraine, orders of the SJA (In accordance with the charter of the SE ICS enterprise, approved by order of the SJA dated 26.11.2019 No. 1142).

The staff and actual number of SE ICS allows for the provision of technical support to SWPs.

SE ICS is provided with qualified personnel who have the following qualifications:

* configuration, installation of server and client parts;
* configuration and operation of applications;
* installation, configuration, provision of data backup and recovery, operation of DBMS;
* installation, configuration and operation of software tools similar to SWPs.

The implementation and operation of SWPs will be carried out on the technical base of SE ICS and with the direct participation of SE ICS administrators.

At the stage of preparing the document "Technical specification" the Supplier must provide requirements for the number and qualifications of SWPs administrators.

All workplaces of authorized persons of HQCJ are equipped with a personal computer with the installed Microsoft Windows operating system, Microsoft Office office suite and software that allows working with documents in PDF format.

HQCJ is provided with the necessary amount of peripheral equipment (printers, scanners, multifunction devices) to perform current functions for verifying subjects and taking into account the functional scope of SWPs.

HQCJ does not have idle (i.e., not fully or partially used by other systems) server capacities, physical data storages, and backup and archive data storage systems that can be used for the operation of SWPs in industrial operation mode. Therefore, such Beneficiary equipment must be taken into account in the overall capacity of SE ICS with the subsequent use of the specified equipment.

Configuration of personal computers, software, and peripheral equipment is carried out by specialists of the HQCJ IT management.

The staff and actual number of the HQCJ IT management allows for technical support of users of the systems currently used by HQCJ and the SWPs being designed.

Number of users of the Software product "Information collection module":

* Number of internal users – up to 500.
* Simultaneous number of users should not be less than 100 with the possibility of scaling.
* Peak number of simultaneous users should not be less than 200 with the possibility of scaling.

Quantitative indicators regarding inspection subjects (estimated for 2025-2026):

* The number of inspection subjects - 10,000.
* The number of family members - 75,000.
* The number of requests to ESoI - 2,000,000.

## Requirements for security

### Requirements for segregation and access control

All end users of SWPs, including administrators, must be individually identified; one user must have no more than one account; rights to an end user must be granted in accordance with a developed role-based access control model.

Tools must be provided for managing user roles. Distribution of user access rights to data must be ensured. When assigning roles to a user in SWPs, the administrator must rely on the existing organizational structure and job responsibilities of the user.

The rights system must be of a "permissive" type, that is, it is considered that the user has only those rights that have been directly granted to him by the administrator. Any attempt to perform an operation for which the rights have not been granted must be blocked.

The rights system must provide the following levels of access separation:

* the ability to delimit access at the entity instance level;
* the ability to delimit access to operations on entities.

### Requirements for authentication and authorization

The secure authentication protocols used should meet industry standards (the encryption protocols used have not been compromised) and best practices.

Login pages should protect all sensitive data entered and should only return a generic error in the event of a login failure.

### Requirements for data encryption and protection

SWPs must provide cryptographic and organizational and technical protection of information in accordance with the requirements of current regulatory legal acts in the field of technical information protection, including the ND TZI of Ukraine.

Information protection at rest:

* Information to be protected must be stored in encrypted form using cryptographic information protection tools (hereinafter – CIPT), which are approved by the State Special Communications Administration for use in state information systems.
* It is recommended to use encryption algorithms implemented in certified CIPT (for example, based on DSTU 7624:2014, GOST 28147-89, or others permitted for use in ITS of the corresponding class).

Information protection in transit:

* Data transfer between SWPs components or with external systems must be carried out with ensuring confidentiality and integrity of information in accordance with ND TZI 2.5-004-99.
* The use of secure communication protocols (TLS 1.2 or newer) is mandatory. Certificates must meet the requirements of current cryptographic standards of Ukraine or be issued by a trusted certification center.
* The use of outdated and vulnerable protocols (SSL, TLS 1.0/1.1) is not allowed.

Key management:

* Keys must be stored in a secure environment that is inaccessible to unauthorized access (e.g., in certified hardware modules or secure storage).
* The use of hard-coded or unprotected keys in software code is prohibited.

Integrity and access control:

* Cryptographic hash functions in accordance with approved standards (e.g., DSTU ISO/IEC 10118 or ND TZI recommendations) should be used to verify data integrity.
* Access to confidential information (including credentials, tokens, and keys) should be implemented in compliance with the principle of least privilege and role-based access control.

General regulations:

* SWPs must have the ability to update cryptographic mechanisms (algorithms, libraries, protocols) in connection with changes in the regulatory framework or the emergence of new requirements from the Beneficiary.
* If it is necessary to use foreign cryptographic tools, their use must be previously agreed with the Beneficiary and comply with the requirements of Ukrainian legislation.

### Requirements for logging and auditing

SWPs should provide event logging.

Changes to security settings (even those made by the administrator) should be logged, tracked, and notified (or configured to do so).

All security events should be logged and timestamped accurately, which should be synchronized using NTP (Network Time Protocol) to ensure accurate timestamp correlation in log sources.

SWPs audit logs should be protected from tampering by SWPs users and administrators.

### Compatibility with antivirus protection and limits of liability

The developed software must be compatible with anti-virus protection tools used on the Beneficiary's infrastructure and not interfere with their functioning. The work of SWPs must be carried out taking into account standard scenarios for checking executable files, network activity and file access.

The presence of anti-virus protection, its configuration, updating and licensing are not included in the scope of this development and are provided by the Beneficiary or the responsible IT infrastructure administrator.

If necessary, the Supplier must provide technical recommendations on exceptions that can be applied in the settings of the anti-virus SW in order to ensure stable operation of the software without reducing the level of information security.

### Other security requirements

Other security requirements:

* Delimitation of access rights to information and operations in SW due to the presence of individual access sets for each user and/or group of users according to their role.
* Ensuring typification of errors that may occur during SW operation.
* Ensuring the development of mechanisms for handling emergency situations. This includes, but is not limited to, the following aspects:
  + error detection and logging,
  + notification of responsible persons or systems,
  + automatic recovery from errors,
  + provision of backup procedures to minimize the impact of errors on the operation of SWPs.
* Ensuring the use of QES overlay and verification tools certified in accordance with the legislation of Ukraine in the field of cryptographic information protection.
* Providing effective security measures to protect against threats such as: cross-site scripting (XSS), SQL injections and others.
* Ensure that critical data (passwords, API keys, certificates, tokens, etc.) is stored outside the code base and configuration files. Industry-standard practices such as secret management systems (e.g., HashiCorp Vault, AWS Secrets Manager, Azure Key Vault) or, at a minimum, environment variables should be used to manage such data. Configuration files can contain references to secrets, but not the secrets themselves in plaintext. Access to the secret store should be strictly limited based on the principle of least privilege.
* Ensure that passwords are stored in a masked form that is not viewable by normal viewers.

Table 1 lists the main security aspects that must be observed when implementing the functional components of SWPs and creating APIs for interaction:

Table 1.

|  |  |
| --- | --- |
| **Security aspect** | **Code security review guide** |
| Security Settings / Permissions | The user's role and permissions are checked on the server. |
| Verification the entered data | Verification of entered data is performed on the server. |
| Injections | User-entered data has been cleaned of unexpected special characters. |
| Special characters and Unicode | User-entered data is stored in its original encoding. |
| Storage of personal data | Personal data is not stored in logs/cache. |
| Shell execution | Shell command arguments and file names are cleaned of unexpected special characters. |
| Data encryption | All data is encrypted during transmission. |
| **API security recommendations:** | |
| Serialization/Data Mapping | Only fields from the "white" list of the data transfer object should be matched. No other fields should be read. |
| Unauthorized API calls | No methods should be allowed for unauthorized users. |
| Cookie attributes | Session tokens must have the attributes "Secure", "HttpOnly", "SameSite", prefix "\_\_Host-". Responses must contain X-Content-Type-Options: nosniff and Strict-Transport-Security: max-age=15724800 |
| Cross-component integration | Integration calls should be properly validated so that a clone of the service cannot publish results like the real service, etc. The source code should not contain hard-coded integration tokens.  For integrated components, the following should be considered:   * Authentication methods; * Secure session control; * Data validation; * Data cleansing. |

## Requirements for ergonomics and technical aesthetics

The user interface should be adaptive: depending on the size of the Internet browser window in which the information is displayed, the sizes, composition and mutual arrangement of interface elements and content should change dynamically.

The main tool for designing the components of the design system should be Figma.

To manage the code base and ensure seamless integration, it is necessary to configure repositories in GitLab with appropriate access policies, pull requests and automatic testing.

The user interface of SWPs should be implemented in Ukrainian.

Information search should be carried out using search indexes that support Cyrillic (Ukrainian) and Latin (English).

All training materials should be developed in Ukrainian.

Documentation developed within the framework of creating SWPs should be provided in Ukrainian.

## Information protection requirements

SWPs must comply with the requirements of regulatory documents on technical information protection.

The creation of a comprehensive information protection system (hereinafter – CIPS) with its state examination and/or obtaining a certificate of compliance with the information security standard SWPs is not the subject of this procurement, but must be performed at the subsequent stages of the construction of UJICS as a whole.

The procurement participant who is awarded the contract is obliged to correct all errors in the software that will be detected at the stage of creating CIPS (obtaining a certificate of compliance with the information security standard), including during the warranty period.

In order to prepare for the creation of a comprehensive information protection system (obtaining a certificate of compliance with the information security standard), the Supplier must prepare and transfer to the Beneficiary a complete set of documentation for the creation of SWPs in accordance with the requirements of the Resolution of the Cabinet of Ministers of Ukraine dated February 21, 2025 No. 205 “Some issues of creating, administering and ensuring the functioning of an informatization tool” (as amended).

Cryptographic libraries for qualified electronic signatures must be used for user authentication. For this purpose, the “IIT User CSK-1” libraries (provided by the Beneficiary) must be used, which must operate as a separate service to which the authentication service will refer.

## Requirements for standardization and unification

In order to ensure compatibility, interoperability, unambiguous interpretation of data and simplify further support, SWPs should be developed in compliance with generally recognized international and industry standards (a detailed list may be specified in agreement with the Beneficiary at the stage of preparing the technical specification).

Standardization of data formats:

All data processed and transmitted by SWPs must comply with the following standards to ensure their unified presentation:

* Date and time: The date and time format must comply with ISO 8601. For data exchange that includes time zones, use RFC 3339. Time zones must be identified according to the IANA Time Zone Database.
* Data exchange formats: The primary format for structured data is JSON (RFC 8259). For tabular data, CSV (RFC 4180) is acceptable.
* Currencies: Currency codes must comply with ISO 4217 (e.g., UAH, USD).
* Countries and regions: Country codes must comply with ISO 3166-1 Alpha-2 or Alpha-3.
* Telephone numbers: Telephone number formats must comply with the international standard ITU-T E.164.
* Units of measurement: Physical quantities and units of measurement must comply with the International System of Units (SI) and ISO/IEC 80000.

Unification of interfaces and documentation:

* API documentation should be developed according to the OpenAPI Specification (OAS) v3.x, which will enable automatic generation of client code and interactive documentation.
* Web services and interfaces should adhere to the W3C (WCAG 2.0) level AA guidelines for accessibility and web standards.

Unification of program code:

* During the development process, uniform rules for naming variables, functions, and components (coding conventions) should be defined and followed.
* Unified approaches to error handling, logging, and configuring system components should be applied.

To ensure maximum compatibility with the existing infrastructure and expertise of the Beneficiary, it is recommended to focus on the following technologies and approaches:

* SW should be built on a client-server architecture using web technologies that do not require additional licensing;
* the client part should be built on standard web technologies that do not require installing additional components on the computer (it is not recommended to use Flash or Java applets);
* JavaScript and cookies support is included;
* Web-Server – Nginx;
* DB - PostgreSQL, MariaDB;
* NoSQL DB - Redis, MongoDB;
* broker- Rabbit or Kafka;
* Front - ReactJS, VueJS;
* Back - Java, NodeJS;
* containerization (Docker) + orchestration (Kubernetes);
* CI/CD - with automatic deployment (Gitlab);
* use of S3 Compatible Object Storage;
* Dashboards - Superset, Grafana;
* Transaction Monitoring – OpenTelemetry;
* User Monitoring - ELK Stack;
* SWPs software servers should be implemented on free Linux-like operating systems;
* all components should be designed with geo-distribution, duplication and horizontal scaling in mind;
* developers are prohibited from or should limit as much as possible the use of the database to run scripts that are not part of the main functionality of the application/service;
* the service availability level should be at least 98.5.

The Bidder may propose alternative technological solutions if they are equivalent or superior in terms of functional, performance or safety characteristics. In such a case, the Bidder's proposal must contain a detailed justification for the choice of alternative technologies and evidence of their compliance with the requirements of these technical requirements.

## Requirements for the reliability of the informatization tool and the preservation of information

### General requirements for reliability

The reliability of an informatization tool is determined by its ability to maintain operability and data integrity under normal and peak load conditions, as well as in the event of hardware or software failures.

Reliability is ensured at the following levels:

1. High Availability Architecture:

* Component redundancy: All critical components of the information and communication system as a whole (application servers, databases, message brokers, load balancers) must be deployed in a fault-tolerant cluster configuration according to a scheme of at least N+1.
* Automatic failover: In the event of a failure of the main component, the system must automatically, without administrator intervention, switch the load to the backup node. The switching time must not exceed the indicators specified in clause 4.7.3.
* Load balancing: the information and communication system as a whole must include software or hardware load balancers to evenly distribute requests between cluster nodes, which ensures stable performance and high availability.

1. Data Integrity and Durability:

* Transactional integrity: Operations that modify related data must be performed within atomic transactions (ACID). This ensures that the operation will either be fully committed or completely rolled back, leaving the data in a consistent state.
* Data replication: For key databases, real-time data replication should be configured to one or more redundant servers, including in a geographically remote data center, to minimize data loss in the event of a disaster (RPO - Recovery Point Objective).
* Backup: A policy for automated data and configuration backups should be implemented. The policy should specify the frequency (full, incremental, differential) and depth of backups. Procedures for restoring from backups should be documented and regularly tested.
* Reliability of information exchange: To guarantee the integrity and completeness of information when exchanged with external systems, control mechanisms (e.g., checksums), data validation against the schema, and delivery confirmation mechanisms (e.g., retry mechanisms, receipts) defined in the relevant exchange protocols must be used.

1. Diagnostics and monitoring:

* Centralized logging: SWPs should maintain detailed logs of events, errors, and operations.
* Error reporting: In the event of an emergency or error, the log should contain comprehensive diagnostic information, including (but not limited to):
  + Exact time of event occurrence;
  + Unique transaction/request identifier;
  + Type and text description of the error;
  + Detailed technical information for diagnostics (e.g. stack trace, execution context);
  + Error severity level.
* Proactive monitoring: The information and communication system as a whole should provide metrics to monitor the status of its components (CPU usage, memory, disk space, number of requests per second, etc.) for early detection of potential problems.

### Reliability criteria

The information and communication system as a whole must operate and be available 24/7 (provide minimal downtime).

SWPs downtime for routine maintenance or disaster recovery should not exceed 8 hours per month on average.

### Disaster recovery

Restoration of availability in the event of a failure for work should not exceed 4 hours. In the event of a failure, the information in the database should remain correct and complete, there should be no loss of data stored in the database.

Mechanisms for recovery after a failure (within the SW SWPs) should be regulated and described by the Supplier.

### Backup and recovery capabilities requirements

The Technical Administrator is responsible for configuring and executing backup procedures in an industrial environment.

Note: Specific parameters, such as the interval between backup/restore procedures, frequency, and location of backup storage (e.g., in two geographically separated data centers), are defined in the operating regulations developed by the Technical administrator based on the documentation and SW capabilities provided by the Supplier.

## Requirements for methods and means of communication for information exchange between the components of the informatization tool

Interaction (information exchange) with other automated systems, information databases and resources should provide the possibility of information exchange (import, export of data) with other automated systems and information resources based on the use of the REST API, SOAP protocol and the implementation of relevant web services. The protocols should be specified at the stage of creating the Technical specification.

Information interaction with other state electronic information resources is carried out by information and communication means in electronic form in accordance with the procedure determined by a joint act of the State Judicial Administration of Ukraine and the relevant state body (institution).

## Requirements for operating modes and productivity of an informatization tool

SWPs should support three main modes of operation:

1. Standard mode:

The main mode in which SWPs operate 24 hours a day, 7 days a week (24/7) and perform all their work processes. This mode provides full availability of all services to users and automated systems within the defined performance indicators.

1. Service (technological) mode:

A mode designed for scheduled maintenance work that cannot be performed in standard mode. The transition to service mode should be planned and accompanied by advance notification of users. The following tasks are performed in this mode:

* Installing software updates.
* Changing the configuration that requires restarting key services.
* Performing routine database maintenance.
* Other work that requires temporary functionality limitations.

During service mode, access to SWPs for end users may be limited or completely suspended.

1. Emergency mode:

The mode into which SWPs automatically enter in the event of a critical failure of one or more components, which makes normal operation impossible. In emergency mode, SWPs must:

* Provide administrators with diagnostic and recovery tools.
* Provide the ability to back up data before starting recovery operations.

Requirements for performance and scalability:

1. System response time:

* Synchronous operations: For interactive user operations and synchronous API requests that do not depend on external systems, the server-side processing time should not exceed 500 milliseconds for 95% of requests under normal load.
* Asynchronous operations: For long-running operations (e.g., requests to external registries), the system should use an asynchronous mechanism. Upon receipt of a request, the system should immediately register it, return a unique identifier and a status of "in process" to the initiator. The initiator should be able to verify the final result of the operation by this identifier.

1. Horizontal scalability:

The SW architecture should be designed according to principles that allow horizontal scaling. The system performance should increase linearly or almost linearly when adding new computing resources (server nodes) without the need to make changes to the program code.

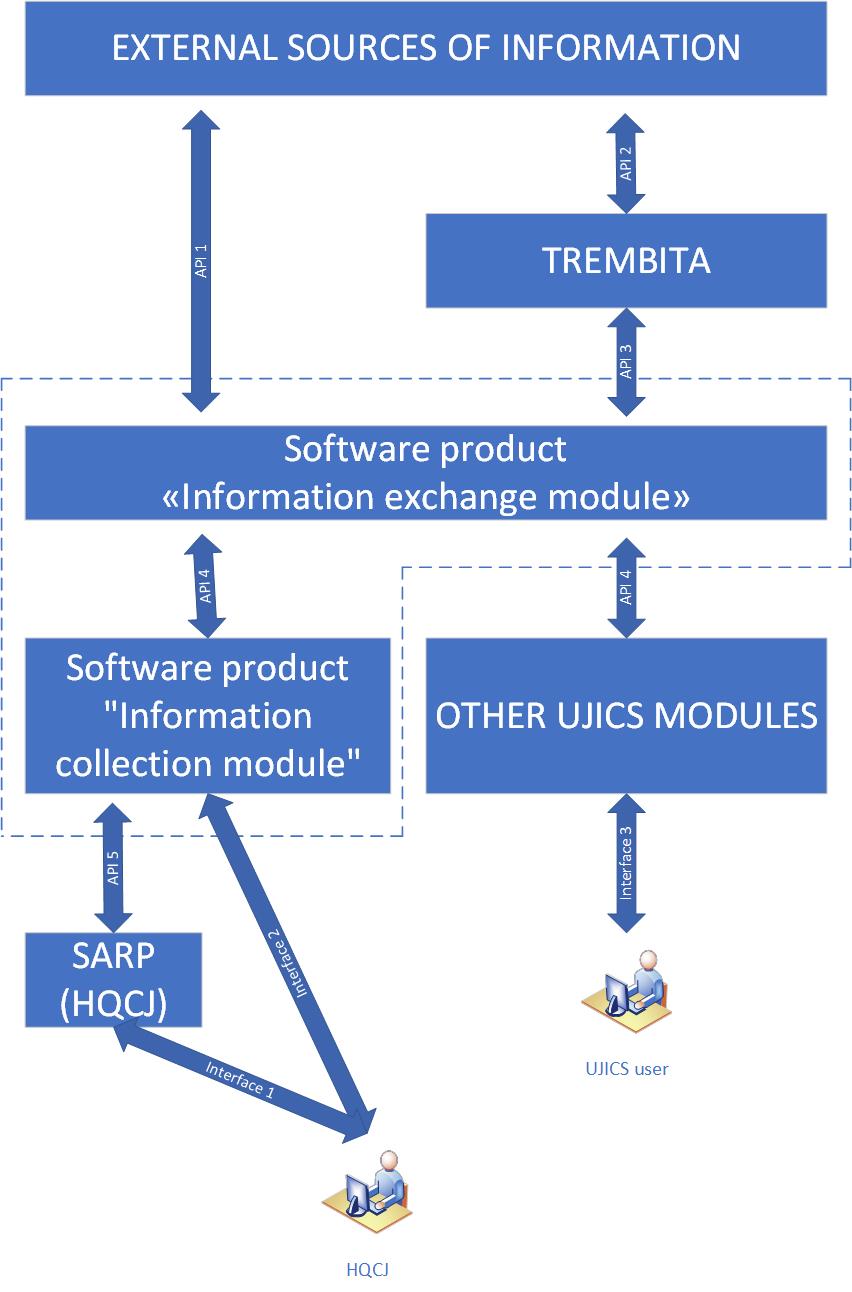
1. Operation under load:

The system must operate stably under peak loads, which may arise from an increase in the number of concurrent users or massive automated requests. The degradation of response time under load must be smooth and predictable.

## Requirements for functions (tasks) performed by an informatization tool

### Approximate principle scheme of the proposed solution

The approximate principle scheme of the proposed solution is given in the following diagram:



Description of the elements of the scheme:

|  |  |
| --- | --- |
| External sources of information | Electronic register - an information and communication system that ensures the collection, accumulation, protection, accounting, display, processing of register data and the provision of register information |
| Trembita | System of electronic interaction of state electronic information resources (Ministry of Digital Transformation of Ukraine) |
| Software product «Information exchange module» | Software product that implements electronic information interaction with external information sources (registers, databases, etc.) |
| Software product «Information collection module» | Software product that implements the collection and processing of information received from ESoI to verify information regarding the compliance of a judge (candidate for the position of a judge) with the rules of professional ethics and the compliance of the judge (candidate for the position of a judge) with the criterion of integrity, including the compliance of the expenses and property status of the judge (candidate for the position of a judge) and his family members. |
| Other UJICS modules | Other specialized software products and modules of UJICS, which implement the initialization of requests through the Software product "Information exchange module" to external sources of information and the analysis of the responses received from them |
| SAPR (HQCJ) | Workflow automation system of the High Qualification Commission of Judges in Ukraine |
| API 1 | Organization of direct access of the Software product "Information exchange module" to external registries using API in accordance with the exchange protocols agreed with the owners of the relevant registries or using the description of the public API |
| API 2 | Organization of access of the Software product "Information exchange module" to external registries using API in accordance with the exchange protocols agreed with the owners of the relevant registries or using the description of the public API provided that "Trembita" is used (this part is outside the Beneficiary segment) |
| API 3 | Organization of access of the software product "Information Exchange Module" to external registers using API in accordance with the exchange protocols agreed with the owners of the relevant registers or using the description of the public API provided that "Trembita" is used (this part is within the SJA segment) |
| API 4 | Initialization of requests through the Software product "Information exchange module" to external information sources and receiving resulting responses from them.  The API must be implemented both for the Software product "Information collection module" directly and for possible use by other software products and modules of UJICS |
| API 5 | Organization of access to the Software product "Information collection module" to initialize the "start" of the inspection for a specific subject of inspection and obtain the results of the automated inspection (list of related parties, responses from state registers, result of the analysis).  Note: revision of the SAPR is not included in the scope of work given in the Technical Requirements and is not performed by the Supplier |
| Interface 1 | Automated workplace of an HQCJ employee for work in SAPR.  Regulated by documentation to SAPR and internal procedures of HQCJ.  Note: revision of the SAPR is not included in the scope of work given in the Technical Requirements and is not performed by the Supplier |
| Interface 2 | Automated workplace of an HQCJ employee for working directly in the Software product “Information collection module”.  Regulated by the documentation for the Software product "Information collection module" and internal procedures of HQCJ.  The user can access the Software product "Information collection module" directly through the Software product "Information collection module" interface for:   * initializing the "start" of the inspection for a specific subject of inspection (batch download is allowed, for example in CSV format) and * obtaining the results of the automated inspection (list of related parties, responses from state registers, result of the analysis) with the ability to search, view, copy and print information, receive (download) documents in agreed formats. |
| Interface 3 | Automated UJICS user workplace for working in the corresponding UJICS software product or module.  Regulated by the documentation for the corresponding UJICS software product or module and the internal procedures of the UJICS owner.  Note: the development of UJICS software products or modules is not included in the scope of work of these Technical Requirements and is not performed by the Supplier. |

Approximate algorithm for generating the results of an automated inspection of a judge (candidate):

1. Initialization of the check: data about the subject of the check (full name, date of birth, individual tax number - here and further the full list of attributes will be specified at the stage of forming the technical specification) is transferred to the Software product "Information collection module" using Interface 2 (including batch loading, for example, in CSV format) and/or API 5 (note: the API 5 format will be specified at the stage of forming the technical specification; this functionality is implemented by the Supplier exclusively within the functionality of the Software product "Information collection module"; revision of the SAPR is not included in the scope of work of these technical requirements and is not performed by the Supplier).
2. Creation of an individual card for each subject of the inspection in the Software product “Information collection module”.
3. Initialization of a request to the Software product “Information exchange module” to obtain information about the family members of the subject of the inspection.
4. The Software product “Information exchange module” contacts the State Register of Civil Status Acts of Citizens of the Ministry of Justice of Ukraine to obtain information about the family members of the subject of the inspection.
5. The Software product “Information collection module” receives information about the family members of the subject of the inspection from the Software product “Information exchange module” and stores it in the Questionnaire of the subject of the inspection. Additionally, taking into account the limited functionality of the API of the State Register of Civil Status Acts of Citizens of the Ministry of Justice of Ukraine, the user is given the opportunity to "manually" enter information about the family members and/or close persons of the subject of the inspection.
6. Initialization of a request to the Software product "Information exchange module" to obtain information from the "Unified Register of Powers of Attorney" about existing powers of attorney of the subject of the inspection and each member of his family, or issued to them.
7. Initialization of a request to the Software product "Information exchange module" to obtain information from an agreed list of state registers about the property status and income of the subject of the inspection, each member of his family and other persons entered in his card.
8. The Software product “Information exchange module” contacts the relevant registers to obtain information from state registers about the property status and income of the subject of the inspection and each member of his family, close persons in accordance with the agreed exchange protocols (including using "Trembita").
9. All received responses are stored in their original form (JSON, etc.) in the Software product database "Information exchange module".
10. The Software product “Information collection module” receives from the Software product “Information exchange module” the information received about the property status and income of the subject of the inspection and each member of his family, close person and stores a certain list of information in the questionnaire of the subject of the inspection (the layout is provided in Annex 1; the list of attributes will be specified at the stage of forming the technical specification) with simultaneous storage of the initial response and a link to the initial response from the state register, which is stored in the Software product “Information exchange module”.

Note: if necessary, the user of the Software product "Information collection module" can view the initial response, but it should be understood that the information format will be "technical", for example, JSON, and not the usual "form", which the user usually receives when accessing the relevant registry using the specialized WEB interface of the relevant registry.

Conditionally, the questionnaire of the subject of inspection will be composed of sections in clear accordance with the number of external registers from which information will be obtained. For example, information about real estate objects will be in a separate section: one object - one line of information. It is proposed to take the form provided in Annex 1 as the basic version of the column for the relevant sections.

1. Obtaining the results of an automated check (list of related persons, responses from state registers, results of the analysis) in the judge's (candidate's) file in SAPR.

Note: the API 5 format will be specified at the stage of forming the technical specification; this functionality can be implemented only if SAPR is upgraded, and is not included in the scope of work according to these Technical Requirements and is not performed by the Supplier.

1. The user receives the results of an automated check (list of related parties, responses from state registers, results of information collection) with the ability to search, view, copy and print information, receive (download) documents in agreed formats directly in the Software product “Information collection module” using the automated workplace of the HQCJ employee.

The proposed implementation scheme based on the modular principle will ensure the possible scaling of the use of the Software product "Information exchange module" by other software products and modules of UJICS.

The list of registers from which there is a need to obtain information is provided in Annex 2.

Note: As part of the implementation of the project, the Supplier must ensure the implementation of information interaction with ESoI, regarding the provision and receipt of data, with the owners of which, at the time of completion of the Technical specification preparation stage, relevant documents (contracts, exchange protocols, etc.) will be signed, which establish legal relations, regarding information interaction.

### General requirements for the functionality of SWPs

To organize effective information exchange, SWPs must perform the process of obtaining and updating reference data necessary to achieve the organization of high-quality information exchange with other software products and modules of UJICS and ESoI.

SWPs must process requests for information exchange in synchronous and/or asynchronous modes, regardless of the server load and the number of requests.

API requirements are extended to exchange interfaces in accordance with the approximate principle scheme (see clause 4.10.1).

Replacement (addition of new) external software products and modules of UJICS and ESoI should not require modification of the API of SWPs, except for the corresponding API that will be changed (added).

SWPs must support API versioning. There should be no situation when a new version of SWPs does not support the previous version of the API, and therefore adaptation of the API of other software products or modules is necessary.

API must provide:

* support for application authorization functions. Authorization should be carried out through the authentication and authorization subsystem using the Token method. One of the authorization protocols should be supported, for example, oAuth;
* support for both synchronous and asynchronous modes;
* provision of multi-threaded operation;
* repeating requests if they were not delivered due to unavailability of the interface.

When exchanging data, the integrity and completeness of the received and sent information must be monitored.

SWPs must be developed using free open source software, such as: PostgreSQL, MySQL or similar. Interaction between the application server and the client for the end user must be performed using the HTTPS protocol (cryptographic protocol).

The creation and further development of SWPs must be carried out in compliance with the Resolution of the Cabinet of Ministers of Ukraine dated February 21, 2025 No. 205 “Some issues of creating, administering and ensuring the functioning of an informatization tool” (as amended), which provides for the use of open technologies, transparency of implementation and the possibility of further scaling and modification of software solutions. Solutions must meet the following general requirements:

* focus on solving critical tasks in order to increase productivity, in particular within the framework of the functioning of the Software product "Information exchange module";
* ensuring high quality, reliability and stability of SWPs, preventing data loss or duplication;
* supporting transparent, standardized and documented integration mechanisms;
* compliance with information and technical security requirements in accordance with current legislation and regulatory documents in the field of information protection;
* ensuring the confidentiality of citizens' personal data in accordance with the requirements of the legislation of Ukraine;
* maintaining a complete history of changes and logging of user actions;
* implementing mechanisms for backing up key SWPs software components;
* openness, transparency and accessibility of the source code of all software components supplied or implemented within the framework of this procurement, in accordance with the terms of licensing free software (Open Source);
* providing a full set of up-to-date supporting and operational documentation.

A general description of the SWPs architecture, indicating the technologies and software tools on the basis of which the SWPs will be built, must be provided by the Supplier as part of the tender offer.

A detailed description and approaches to the implementation of the SWPs must be formed by the Supplier at the stage of "Development of the technical specification" based on the information provided by the Beneficiary.

### General requirements for the Software product "Information exchange module"

The Software product “Information exchange module” provides efficient, unified and secure interaction between UJICS and ESoI software products and modules.

The main aspects of the purpose of the Software product "Information exchange module":

* Integration and interaction:
  + Providing mechanisms for connecting new information services and organizing their interaction with ESoI.
  + Providing the possibility of electronic interaction between software products and modules of UJICS and ESoI, in particular through unified APIs.
* Management of information flows:
  + Coordination and management of electronic interaction between UJICS and ESoI software products and modules.
  + Providing requests from UJICS software products and modules to ESoI.
  + Normalization of ESoI data according to the requirements of UJICS software products and modules.
  + Transmission of responses from ESoI to UJICS software products and modules.
* Functionality for data integration and exchange:
  + Providing automated data exchange, including support for requests, responses, and data normalization.
  + Support for the use of modern data exchange protocols and formats (REST API, JSON, XML).
  + Ability to configure integration parameters to adapt to changes in authentication and interaction parameters.
* Autonomy and technological capability:
  + Activity as an autonomous technological SWPs UJICS, which can function independently, ensuring the reliability and stability of the entire system.
  + Support scalability and adaptability for increasing data volumes and the number of users.
* Provision of a single information space:
  + Building an integrated Software product for centralized data storage, processing and exchange.
  + Maintaining the integrity, relevance and reliability of data during its use.

Thus, the Software product "Information exchange module" is a key element of UJICS, which ensures the integration, management and coordination of information flows to increase the efficiency of interaction between the judiciary, state bodies and other external entities of electronic interaction.

Within the framework of these technical requirements, the Software product "Information exchange module" must implement electronic interaction in accordance with the exchange protocols agreed upon by the Beneficiary with the owners of the relevant registers or using the description of the public API:

* with all UJICS subsystems that are ready at the time of SWPs launch and the term of its warranty service (API 4 - described in detail in p.4.10.1);
* with IS, registers, databases of state bodies, local governments, international organizations, business entities and law enforcement agencies of other states, including those carried out using the system of electronic interaction of state electronic information resources "Trembita" (API 3 - described in detail in p.4.10.1);
* in the absence of technical possibility of data transmission using the system of electronic interaction of state electronic information resources "Trembita", electronic information interaction of subjects of electronic interaction can be carried out using other information and communication systems with the use of appropriate comprehensive information protection systems with confirmed compliance according to the results of state expertise in the manner established by law (API 1 - described in detail in p.4.10.1).

The goals of creating the Software product "Information exchange module":

* Centralization of management of information interactions:
  + Creation of a single UJICS element to coordinate all integration processes between UJICS and ESoI software products and modules.
  + Provision of a unified data exchange mechanism through a single access point.
* Unification and normalization of data:
  + Implementation of data normalization mechanisms.
  + Ensuring high quality and integrity of data in the process of information interaction.
* Automation of the management of information interactions:
  + Implement automated routing of requests between systems based on their specifications and priorities.
  + Support for asynchronous request processing to improve system performance.
* Scalability and adaptability:
  + Building a Software product that scales easily to handle growing volumes of requests and new information interactions.
  + Configuring information interaction rules to quickly adapt to changing requirements.
* Increasing the security of information interactions:
  + Implementation of modern authentication and authorization mechanisms (OAuth, JWT).
* Monitoring and management:
  + Integration of monitoring systems to identify problems in the operation of the Software product.
  + Providing administrators with tools for performance analysis and troubleshooting.
* Extension of UJICS functionality:
  + Providing a flexible platform for integrating new services and subsystems in the future.
  + Support API versioning to minimize the impact of changes on existing integrations.

The Software product “Information exchange module” must implement the following functionalities:

* Support of standard protocols and formats:
  + Core stack: The use of RESTful web services with JSON data format is a priority. The system must support standard HTTP methods (GET, POST, PUT, PATCH, DELETE).
  + Compatibility with other systems: For interaction with existing or specific systems, the ability to work with the SOAP protocol (using XML) and other data formats (e.g., CSV, XML) must be provided. The ability to transform data between different formats must be architecturally built in.
  + Data transfer security: All interaction (except if the interaction is implemented using the National Confidential Communication System) with external systems must occur exclusively using the secure HTTPS protocol.
* Architectural flexibility and extensibility:
  + Modular adapters (connectors): The architecture of the Software product "Information exchange module" should allow the development and connection of specific adapters for integration with various external information systems. Each adapter should encapsulate the logic of interaction with a specific external API, including authentication, authorization and data transformation.
* Flexible mechanisms for initiating exchange. The Software product “Information exchange module” must support various methods for initiating data exchange:
  + Scheduled: Execution of scheduled tasks for periodic data exchange (for example, every night).
  + Event-driven: Initiation of real-time exchange upon the occurrence of a certain event in one of the systems (API 4).
  + User-driven: Ability to manually start the exchange via the administrator interface.
* Audit and performance control:
  + Detailed logging: Logging of each exchange operation with key parameters: transaction ID, start and end time, execution status (success/error) and error message.
  + Automatic notification (alert): Setting up automatic notifications for responsible administrators in case of unsuccessful data export/import operations to ensure quick response to incidents.

### Functional requirements for the Software product "Information exchange module"

The Software product “Information exchange module” performs electronic interaction in accordance with the exchange protocols agreed upon by the Beneficiary with the owners of the relevant registers or using the description of the public API.

The following is a typical example of information interaction between the Software product "Information exchange module" and ESoI.

According to the automated exchange protocol, the Software product "Information exchange module" sends http requests for providing information in JSON or CSV or XML format (text formats for presenting tabular data) to ESoI. The result of the request is a file in JSON\CSV\XML format of the same structure.

The attributes of such a file are:

* request identifier;
* request data encrypted using the CSK user library "Signature (PHP extension module)";
* QES on the request data.

Information exchange is carried out with the imposition of a qualified electronic signature and information encryption using the CSK user library "Signature (PHP extension module)" of the user software complex of the key certification center "IIT User CSK-1" (provided by the Beneficiary).

The exchange process is divided into several parts, namely: data preparation, data sending, checking the status of requests, data receipt.

Exchange with ESoI is organized in the form of drivers (connectors) for exchange with ESoI, according to the relevant exchange protocols approved by the Beneficiary.

**Data preparation**

The start of each part of the Software product "Information exchange module" is carried out using the task scheduler, which calls the corresponding part of the exchange functionality, which are in the Software product controller.

Data preparation begins with the exchange component, in which the list of drivers (connectors) and their settings are loaded, a list of data that requires the formation of requests in ESoI is loaded. The data for which it is necessary to make a request for information search to ESoI is transferred to the corresponding drivers (connectors), in which requests to ESoI are formed in the required format, according to the exchange protocols.

For each request, a record with exchange parameters is formed in the Software product "Information exchange module" database.

Data exchange methods implement the mechanism for sending and receiving data:

* sending request data to a specified address or link;
* controlling response codes;
* receiving and generating request headers;
* supporting authorization and authentication.

Parts of the exchange, such as sending data, checking the status and receiving data, depend on ESoI and are implemented according to the exchange protocol. Exchange with ESoI works according to different protocols, so some parts of the exchange system may not be involved.

In case of receiving requests for access to data containing personal data of users, the Software product "Information exchange module" must ensure the recording of each such request. The record must contain: the requester's identifier, the type of requested data, the purpose of the request and the date/time of processing, in accordance with the requirements for transparency of personal data processing, in accordance with the Law of Ukraine "On Personal Data Protection". All operations with personal data must be recorded in event logs that provide access auditing and control of compliance with legislative norms. The storage of such records must meet information security requirements, in particular regarding limiting access to authorized persons only.

**Checking the status of requests**

The Software product “Information exchange module” should allow initiators (UJICS software products and modules) of the request to check the status of the sent request, as well as provide the ability to resend the request in cases of ESoI failures.

**Receiving data**

The Software product “Information exchange module” must process requests from UJICS software products and modules to obtain data in cases where:

* A UJICS user, in order to perform his/her duties, needs to check the relevance of the data specified in UJICS entities;
* A UJICS user, in order to perform his/her duties, needs to create an entity in UJICS based on relevant data received from other ESoIs;
* In other cases, which may be additionally described at the stage of creating the technical specification.

The Software product “Information exchange module” should provide unification, typification and coding of the same type of information that can be used by a large number of users, regardless of their role in UJICS.

The Software product “Information exchange module” should provide the ability to view responses from other systems and state registers that have been received in the form of JSON files with one or more entities, or in the form of generated documents, depending on the ESoI request processing algorithms.

The Software product “Information exchange module” should provide the ability to specify values in the set of filtering parameters allowed for the corresponding ESoI requests, for the convenience of searching for specific requests/responses.

To simplify and optimize the work of users, the Software product “Information exchange module” should provide them with the ability to obtain information about ESoI necessary for creating entities within UJICS, for example, a description of the exchange protocol, etc.

**Processing and temporary storage of received data**

After receiving a data set from ESoI, the Software product "Information exchange module" must automatically perform the conversions necessary for the data to be used by the request initiator (UJICS software products and modules).

The Software product "Information exchange module" must store the data received from ESoI in its pure form only for a certain time specified in the settings of the Software product "Information exchange module".

The procedure and terms of temporary storage of the received data and their deletion from the Software product "Information exchange module" database must be additionally agreed between the Supplier and the Beneficiary at the stage of "Development of the technical specification".

**Data structure**

System data must be presented in a structured form.

The data structure must clearly define the rules for storing information to ensure accurate identification of data in the Software product “Information exchange module”, if this is determined by the business process of working with data.

**Data organization**

The organization of data in the Software product “Information exchange module” should ensure holistic, efficient and unified management of all information necessary to perform applied tasks:

* information arrays should be unified and used together for all functional tasks of the Software product "Information exchange module";
* the data structure should be optimized to ensure minimal costs for storage, access, processing and changes.

**Logging**

The Software product “Information exchange module” must ensure the collection and storage of all types of logs, the main ones being:

* service logs (registration, authorization, authentication, information interaction);
* system logs (operating system, configuration changes, failures, deployment of new services, metrics);
* security logs;
* user action logs (data versioning, recording of changes with indication of the person who entered or changed the data).

Software product "Information exchange module" should provide logging and event logging.

In case of emergency situations or errors, diagnostic tools should record the necessary information to identify the problem.

Diagnostics and information processing should be carried out for each component of the subsystem and its work processes.

All transactions should have unique numbers, in case of incorrect transaction processing, the number and error should be recorded in the event log.

**Automatic logging of interactions with ESoI**

The Software product “Information exchange module” automatically records interactions with ESoI.

Changes in the status of work, components and errors that occur during their operation are also recorded.

All logging events must be registered and accurately timed using NTP (network time protocol) to ensure the exact ratio of time stamps in the log logs.

Only a user with appropriate access rights should be able to view log files.

The list of logs provided is not exhaustive. A detailed list of logs to be stored in the Software product “Information exchange module”, as well as their storage period, must be additionally agreed between the Supplier and the Beneficiary at the stage of “Development of the technical specification”.

**Requirements for the role model**

Requirements for the role model of the Software product "Information exchange module" must be verified by the Supplier and agreed with the Beneficiary at the stage of developing the technical specification.

The user authentication and authorization service uses QES, which ensures verification of user access to the functionality of the Software product "Information exchange module".

Upon successful authorization, the user enters the Software product "Information exchange module".

The user profile page must be able to view the user profile under which the Software product "Information exchange module" was entered, displaying information about the user and his contact details.

Main roles:

* Administrator

Responsibilities:

* + Managing users, their roles and access rights.
  + Configuring API parameters (keys, URLs, timeouts, security policies).
  + Monitoring system status, logs and journals.
  + Solving technical problems and responding to incidents.
  + Defining general parameters of the Software product "Information exchange module".

Access level:

* + Full access to all functional components of the system.
  + Ability to make changes to API configuration and system settings.
* Integration manager

Responsibilities:

* + Setting up and supporting integrations with ESoI.
  + Managing requests to ESoI.
  + Coordination of integration projects with internal (UJICS) and external systems (ESoI).

Access level:

* + Access to integration services settings.
  + Limited access to request and response logs.
* Request initiator (according to the agreed API 4; see section 4.10.1)

Responsibilities:

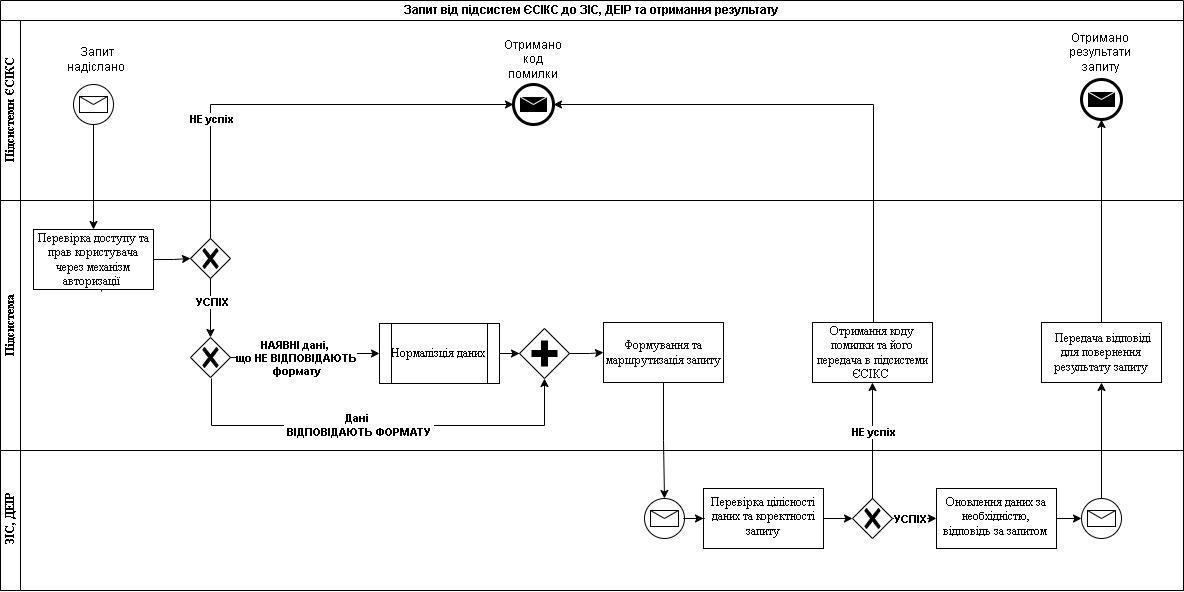
* + Interaction with the Software product “Information exchange module” through the interfaces of external systems.
  + Providing the necessary requests to the Software product "Information exchange module" or obtaining data.

Access level:

* + Access to specific APIs that are limited by the context of their use.

**Basic workflow Request from UJICS to ESoI**

The basic workflow of requesting from UJICS to ESoI and receiving the result is provided in the following figure (in Ukrainian):



**Subprocesses of the work of the Software product "Information exchange module"**

1. Request initialization

Participants:

* other UJICS software products and modules.

Actions:

* Forming a request using API 4 through the user interface of the corresponding UJICS software products and modules.
* Verifying access and rights to API 4 through the authorization mechanism (OAuth, JWT).

Result:

* Successful authorization and request initialization.

1. Submitting a request

Participants:

* API system.

Actions:

* Receiving an API request.
* Verifying data integrity and correctness of the request.
* Routing the request to the appropriate internal component of the Software product "Information exchange module" for processing.

Result:

* The request has been accepted and forwarded for processing.

1. Request processing

Participants:

* Software product «Information exchange module» and ESoI.

Actions:

* Normalization (preparation of data formats for requests to ESoI) of data:
  + Transform the query data structure into a format that meets the standards of the target ESoI.
  + Validate the data to ensure it meets specifications.
* Interaction with target systems:
  + Execution of requests to ESoI.
  + Receiving and processing responses.

Result:

* Data normalized, response received, updated in the Software product “Information exchange module”.

1. Returning the result

Participants:

* Software product «Information exchange module».

Actions:

* Forming a response based on the results obtained.
* Sending the response to the initiator (UJICS software products and modules).
* Logging actions in the Software product “Information exchange module” to ensure transparency.

Result:

* Response returned to initiator.

1. Monitoring and management

Participants:

* System administrator, Integration manager.

Actions:

* Monitoring API performance through appropriate tools (event logs).
* Analysis of query performance.
* Detection and resolution of incidents (errors, crashes, etc.).

Result:

* Continuous support of the stability of SW operation.

**Requirements for the Software product "Information exchange module" user account**

The user account of the Software product "Information exchange module" is a web page that displays the functionality of the Software product "Information exchange module", available to the user according to the role model and access rights.

General requirements for user accounts:

* Adaptability:
  + The user interface should be user-friendly on workstations.
* Security:
  + Use HTTPS to encrypt data in transit.
  + Session control with automatic logout after a period of inactivity.
* Action logging:
  + All actions in user accounts must be logged with time, user, and result.
* Personalization:
  + User accounts should allow customization of the interface according to user needs (filters, sorting).
  + The structure of user accounts should ensure the separation of access according to roles, convenience in performing tasks, and compliance with security standards.

Based on the proposed role model, user accounts should provide access to functionality according to the role, maintain usability, and meet applicable security standards. Below are the basic requirements for each role:

1. Administrator user account

Functionality:

* Manage user roles and access rights.
* Configure API parameters (keys, URLs, timeouts, access policies).
* View logs of user actions and system events.
* Configure security.
* Monitor API performance and system health
* Incident response tools.

Interface:

* Intuitive dashboard with graphs and system status indicators.
* Module for viewing and filtering event logs.
* Panel for quick access to security settings.

1. Integration manager user account

Functionality:

* Configuring integrations with ESoI.
* Viewing the status of requests and responses.
* Making changes to integration parameters (connectors, adapters, exchange protocols).
* Forming and managing ESoI request queues.

Interface:

* List of active integrations with the ability to edit.
* Visualization of integration status (success of requests, delays, failures).
* Message panel about errors or disruptions in the work of integrations.

For ease of use of the Software product “Information exchange module”, the following functions must be implemented, which are available in all sections:

* Sorting tables (when displaying information in tabular form);
* Selecting the number of records to display on a page (when displaying information in tabular form);
* Page navigation (when displaying information in tabular form);
* Displaying error messages in case of incorrect filling in of fields in forms.

### General requirements for the Software product "Information collection module"

Software product "Information collection module" provides creation and review of requests to ESoI.

The main aspects of the purpose of the Software product "Information collection module":

* Information flow management:
  + Initialization to the Software product "Information exchange module" of requests to the ESoI to collect information about the inspection subjects.
  + Receiving from the Software product "Information exchange module", processing, grouping and storing responses to requests to ESoI.
  + Normalization of ESoI data in accordance with the requirements for accounting for information about the subjects of inspection.
* Functionality for integration and data exchange:
  + Providing automated data exchange, including support for requests, responses, and data normalization.
  + Support for the use (storage, upload, processing) of modern data exchange protocols and formats (REST API, JSON, XML).
  + Ability to configure integration parameters to adapt to changes in authentication and interaction parameters.
* Ensuring a single information space:
  + Maintaining the integrity, relevance and reliability of data during its use.

Within these technical requirements, the Information collection module must implement electronic interaction:

* at the stage of initializing the request to the Software product "Information collection module", data about the subject of the inspection (full name, date of birth, individual tax number - here and further the full list of attributes will be specified at the stage of forming the technical specification) is transferred using Interface 2 (including batch loading, for example, in CSV format) and/or API 5 (note: the API 5 format will be specified at the stage of forming the technical specification; this functionality is implemented by the Supplier exclusively within the functionality of the Software product "Information collection module"; SAPR modernization is not included in the scope of work of these technical requirements and is not performed by the Supplier);
* receiving the resulting responses from the Software product "Information exchange module".

The Software product “Information collection module” must provide:

* Use of files of the agreed API4 format for information exchange with the Software product “Information exchange module” (formats will be agreed between the Supplier and the Beneficiary at the stage of developing the technical specification).
* Ability to configure routine data exchange, or upon the occurrence of certain events;
* Maintaining data exchange logs with recording of the main parameters (date, time of start and end of package execution, execution status);
* Provide the ability to save information about the subjects of inspection in the database Software product “Information collection module”;
* Management of security and access policies to services and data.

### Functional requirements for the Software product "Information collection module"

According to the automated exchange protocol, the Software product "Information collection module" sends requests and receives the results of requests in an agreed (API4) format.

The mandatory attributes of such requests are:

* request identifier;
* request data encrypted using the CSK user library "Signature (PHP extension module)";
* QES on the request data.

Information exchange is carried out with the imposition of a qualified electronic signature and encryption of information using the CSC user library "Signature (PHP extension module)" of the user software complex of the key certification center "IIT User CSC-1" (provided by the Beneficiary).

The work of the information collection system is divided into several parts, namely: data preparation, sending data, checking the status of requests, receiving data.

Exchange with ESoI is organized exclusively through the Software product "Information exchange module".

**Data preparation**

The collection of information for a specific subject of inspection begins with the entry of key data for this subject of inspection:

* Full name;
* date of birth;
* individual tax number;
* reason for the request.

Additionally, given the limited functionality of the API of the State Register of Civil Status Acts of Citizens of the Ministry of Justice of Ukraine, the user is given the opportunity to “manually” enter information according to the above list of attributes about family members and close persons of the subject of the inspection. Since requests to ESoI for each family member and close persons of the subject of the inspection are initiated separately, adding “new” family members and close persons of the subject to the list to obtain information about them from ESoI is allowed at any stage of collecting information about the subject of the inspection.

The work of the Software product “Information collection module” is carried out using the task scheduler, which calls the corresponding part of the exchange functionality.

Data about the subjects of the inspection, their family members and close persons, for whom it is necessary to make a request to search for information in ESoI, is transferred to the Software product “Information exchange module”, according to the exchange protocols (API4).

For each request, a record with exchange parameters is formed in the database.

In case of receiving requests for access to data containing personal data, the Software product "Information collection module" must ensure the recording of each such request. The record must contain: the requester's identifier, the type of requested data, the purpose of the request and the date/time of processing, in accordance with the requirements for the transparency of personal data processing, in accordance with the Law of Ukraine "On Personal Data Protection". All operations with personal data must be recorded in event logs that provide access audit and control of compliance with legislative norms. The storage of such records must meet the requirements of information security, in particular regarding the restriction of access to authorized persons only.

**Checking the status and managing the information collection process**

The Software product “Information collection module” should allow users to check in real time the overall status of the information collection process for a subject, as well as the detailed status of requests to each individual register (e.g., "in progress", "successfully completed", "error").

In the event of a mass failure, when a significant part of the requests to the registers were not completed, the user should be able to initiate a restart of the entire information collection process for a specific subject. The Software product “Information collection module” should be intelligent enough to resend only those requests that were not successfully completed earlier.

To speed up the work when conducting periodic or repeated checks, the Software product “Information collection module” should provide functionality for creating a new information collection process based on the data of the existing one. When using this function, the system should create a new, "clean" check, automatically copying into it all the original data about the subject of the check and the persons related to it (name, individual tax number, data on family members, etc.). The user will only have to initiate a new start of information collection.

**Receiving data**

The Software product “Information collection module” must process requests for data in cases where:

* To perform job duties, the user must check the relevance of the data specified in the entities of the Software product "Information collection module";
* To perform job duties, the user must create an entity in the Software product “Information collection module” based on the relevant data received from the Software product "Information exchange module";
* In other cases that may be additionally described at the stage of creating the technical specification.

The Software product “Information collection module” should provide unification, typification and coding of the same type of information, which can be used by a large number of users, regardless of their role in the Software product “Information collection module”. The Software product “Information collection module” should provide users with the ability to view responses from other systems and state registers, which were received in the form of JSON files with one or more entities, or in the form of generated documents, depending on the ESoI request processing algorithms.

**Processing and temporary storage of received data**

After receiving a data set from the Software product "Information exchange module", the Software product "Information collection module" must automatically perform the conversions necessary for the use of data by users of the Software product "Information collection module".

The Software product "Information collection module" must store the data received from the Software product "Information exchange module" in its pure form only for a certain period of time specified in the settings of the Software product "Information collection module" (the storage period will be specified and agreed with the Beneficiary at the stage of preparing the technical specification).

**Data structure**

System data must be presented in a structured form.

The data structure must clearly define the rules for storing information to ensure accurate identification of data in the Software product "Information collection module", if this is determined by the data workflow.

**Principles of working with data**

Working with data in the Software product "Information collection module" must comply with the following principles:

* integrity and continuity: data must maintain logical integrity, be consistent and consistent during processing, transmission and storage;
* reliability and security: data protection from loss, damage (corruption) and unauthorized access must be ensured, including means of backup and access control;
* relevance and accuracy: mechanisms for constant control over the reliability and updating of data must be implemented;
* uniformity and standardization: data must comply with established formats and standards, be unified to ensure compatibility;
* flexibility of use: although the data must be uniform within the Software product "Information collection module", the architecture must allow their adaptation to various application tasks;
* adaptability to changes: the Software product "Information collection module" must be able to adapt to changes in requirements and data sources without disrupting the overall stability of work;
* error minimization: validation and control tools should be implemented to reduce the likelihood of errors during data input, processing and output.

**Data organization**

Data organization should ensure the unity and storage of all necessary information to solve problems.

Information arrays should be uniform for all functional tasks of the Software product "Information collection module".

The data structure should be optimized to ensure minimal storage, access, processing and modification costs.

**Logging**

The Software product “Information collection module” must ensure the collection and storage of the following logs:

* service logs (registration, authorization, authentication, information interaction);
* system logs (operating system, configuration changes, failures, deployment of new services, metrics);
* security logs;
* user action logs (data versioning, recording of changes with indication of the person who entered or changed the data).

Software product "Information collection module" should provide logging and event logging.

In case of emergency situations or errors, diagnostic tools should record the necessary information to identify the problem.

Diagnostics and information processing should be carried out for each component of the subsystem and its work processes.

All transactions should have unique numbers, in case of incorrect transaction processing, the number and error should be recorded in the event log.

**Automatic logging of interactions with external systems**

The Software product “Information collection module” automatically records interactions with the Software product “Information exchange module”.

Changes in the status of work, components and errors that occur during their operation are also recorded.

All logging events must be registered and accurately timed using NTP (network time protocol) to ensure the exact ratio of time stamps in the log logs.

A user with appropriate access rights must be able to view log files.

A detailed list of logs to be stored in the Software product “Information collection module”, as well as their storage period, must be additionally agreed between the Supplier and the Beneficiary at the stage of “Development of the technical specification”.

**Requirements for the role model**

The user authentication and authorization service uses QES, which ensures verification of user access to the functionality of the Software product "Information collection module".

Upon successful authorization, the user enters the Software product "Information collection module".

The user profile page should provide a view of the user profile under which the Software product "Information collection module" was logged in, displaying information about the user, his contact details and the ability to change the password.

Main roles:

* Administrator

Responsibilities:

* + Managing users, their roles and access rights.
  + Configuring API parameters (keys, URLs, timeouts, security policies).
  + Monitoring system status, logs and journals.
  + Solving technical problems and responding to incidents.
  + Defining general parameters of the Software product "Information collection module".

Access level:

* + Full access to all functional components of the system.
  + Ability to make changes to API configuration and system settings.
* User-SAPR (in accordance with the agreed API 5; see clause 4.10.1; subject to SAPR Beneficiary modernization; SAPR modernization is not included in the scope of work of these Technical Requirements and is not performed by the Supplier)

Responsibilities:

* + Interaction with the Information Collection Module via external interfaces (API5).
  + Providing the necessary requests to the Software product "Information collection module" (to initialize the "start" of the inspection for a specific inspection subject) or obtaining automated inspection data.

Access level:

* + Access to specific APIs5 that are limited by the context of their use.
* User-HQCJ

Responsibilities:

* + Interaction with the Software product "Information collection module" via the Software product "Information collection module" interface (Interface 2; see section 4.10.1) for:
    - initializing the "start" of the inspection for a specific subject of inspection (batch download is allowed, for example in CSV format) and
    - obtaining the results of the automated inspection (list of related parties, responses from state registers, result of the analysis) with the ability to search, view, copy and print information, receive (download) documents in agreed formats.

Access level:

* + Entering key data on a given subject of the inspection, including family members of the subject of the inspection;
  + Full access to view information on the subject of the inspection;
  + Minimum level of access to functions related to their work.
* User-HQCJ (browsing only)

Responsibilities:

* + Interaction with the Software product “Information collection module” via the Software product “Information collection module” interface (Interface 2; see section 4.10.1) for:
    - obtaining the results of an automated check (list of related parties, responses from state registers, results of the analysis) with the ability to search, view, copy and print information, receive (download) documents in agreed formats.

Access level:

* + Full access to view information on the subject of the inspection;
  + Minimum level of access to functions related to their work.

**Subprocesses of the Software product "Information collection module"**

1. Request initialization

Participants:

* User-SAPR
* User-HQCJ.

Actions:

* initializing the "start" of the inspection for a specific subject of inspection.

Result:

* Successful authentication and authorization, request initialization.

1. Transfer request

Participants:

* API4 (Software product «Information exchange module»).

Actions:

* Checking data integrity and query correctness.
* Sending API4 query to Software product "Information exchange module".

Result:

* The request has been submitted for processing.

1. Request processing

Participants:

* API4 (Software product «Information exchange module»).

Actions:

* Normalization (preparation of data formats for requests to ESoI) of data:
  + Receiving and processing responses;
  + Converting the response data structure into a format that meets the standards of internal processes (Interface 2) or target external systems (API5).
  + Validating data to ensure it meets specifications.
* Interaction with target internal processes:
  + Initialization of requests in case of receiving information about “new” family members of the subject of the inspection.

Result:

* Data is normalized, retrieved, or updated in the target system.
* Initiated requests in case of receiving information on "new" family members of the subject of the inspection.

1. Returning the result

Participants:

* Software product «Information collection module».

Actions:

* Formation of consolidated information based on the results obtained.
* Transmission of the response to the user (Interface 2) or the initiating system (in accordance with the agreed API 5; see clause 4.10.1; subject to SAPR modernization by the Beneficiary; SAPR modernization is not included in the scope of work of these Technical Requirements and is not performed by the Supplier).
* Logging of actions in the system to ensure transparency.

Result:

* Response returned to initiator.

1. Monitoring and management

Participants:

* System administrator.

Actions:

* Monitoring API performance through appropriate tools (dashboards, event logs).
* Analysis of query performance.
* Detection and resolution of incidents (errors, crashes, etc.).

Result:

* Continuous support of the stability of the work of the Software product "Information collection module".

**Requirements for the user account Software product "Information collection module"**

The user account Software product "Information collection module", is a web page that displays the functionality of the Software product "Information collection module", available to the user in accordance with the role model and access rights.

General requirements for user accounts:

* Adaptability:
  + The user interface should be user-friendly on workstations.
* Security:
  + Use HTTPS to encrypt data in transit.
  + Session control with automatic logout after a period of inactivity.
* Logging actions:
  + All actions in the offices must be logged with the time, user, and result.
* Personalization:
  + User accounts should allow customization of the interface according to user needs (filters, sorting).
  + The structure of user accounts should ensure the separation of access according to roles, convenience in performing tasks, and compliance with security standards.

Based on the proposed role model, user accounts should provide access to functionality according to the role, maintain usability, and meet applicable security standards. Below are the basic requirements for each role:

1. Administrator user account

Functionality:

* Manage user roles and access rights.
* Configure API parameters (keys, URLs, timeouts, access policies).
* View logs of user actions and system events.
* Configure security.
* Monitoring API performance and system status
* Tools for responding to incidents.

Interface:

* Intuitive dashboard with graphs and system status indicators.
* Module for viewing and filtering event logs.
* Panel for quick access to security settings.

1. User account User-HQCJ

Functionality:

* Review the status of requests and responses.
* Review and make (if authorized) changes to the list of inspection subjects and their family members.

Interface:

* List of inspection subjects with the ability to edit (provided you have permissions).
* Visualization of inspection status (success of requests, delays, failures).

For ease of use of the Software product “Information collection module”, the following functions must be implemented, which are available in all sections:

* Sorting tables (when displaying information in tabular form);
* Selecting the number of records to display on a page (when displaying information in tabular form);
* Page navigation (when displaying information in tabular form);
* Displaying error messages in case of incorrect filling in of fields in forms.

For the convenience of users in processing the information received from ESoI about the subject of the inspection, his family members and close persons, and taking into account the specifics of each ESoI, the information card on the subject of the inspection should be formed according to the relevant sections (an approximate layout is provided in Annex 1; the final form should be specified at the stage of preparing the technical specification) according to the following principles:

* first section – information about the subject of the inspection;
* second section – a list of family members and close persons of the subject of the inspection (tabular form; one line – one family member);
* each subsequent section – corresponds to a separate ESoI (see p.4.10.1):
  + tabular form;
  + one line – one response from ESoI;
  + the ability to view the received response in its original form (JSON, etc.);
  + if technically possible, the ability to view the received response in the form of a visual representation (with saving in PDF) with the main fields of the original response.

# Requirements for development and transfer of services

## Requirements for the development

During the design of the SWPs architecture, the Supplier shall provide indicative hardware requirements that will be required to run the SWPs (in test and production environments, including data backup requirements) taking into account the performance requirements set out in this document.

Upon completion, the Supplier shall provide the Beneficiary with the final hardware requirements that will be required to operate the SWPs taking into account the performance requirements set out in this document.

An indicative schedule for the implementation of the SWPs life cycle stages (design, development and implementation) is provided in Annex 3.

Requirements for potential Suppliers are provided in Annex 4.

## Requirements for the transfer of services

### Requirements for the order of deployment

SW deployment involves several stages of work:

* Development or adaptation of the software.

At this stage, the Supplier develops SWPs, selects, adapts and (or) links the purchased software, develops software documentation in accordance with the requirements of current legislation, including the documents "Test program and methodology", "Installation (deployment) instructions" and "User manual (respectively for each role)".

* Deployment of hardware and SW.

At this stage, the Technical Administrator installs and configures the necessary components of the general system software, (if necessary) development tool environments in the test (if available) and industrial SW environment, configuration management tools. Installation of the developed SW or its component in the formed environment in accordance with the document "Installation (deployment) instructions" and processing (testing) of identified problems.

* Preparing the Technical Administrator and Beneficiary for the implementation of SWPs.

At this stage, work is being carried out on the organizational preparation of the automation facility for the introduction of SWPs into operation, including:

* + Implementation of project solutions in accordance with the organizational structure of the Technical Administrator and Beneficiary.
  + Providing the Technical Administrator and Beneficiary units with instructional and methodological materials.
  + Implementation of information classifiers.
* Staff training.

At this stage, personnel training and verification of their ability to ensure the functioning of SWPs are carried out.

The Supplier is obliged to conduct training for the employees of the Beneficiary and the Technical Administrator:

* + The administrator training plan should contain theoretical and practical tasks on installing and operating software components, diagnosing and eliminating typical errors (malfunctions) that may occur during the operation of SWPs.
  + User training should include studying the functionality and procedure for working with SWPs.
  + For all types of training, the following should be developed and used:
    - Training programs.
    - Presentations.
    - User guides for each role.
  + All training materials must be developed in Ukrainian and available in electronic format.
  + The duration of training is 24 hours for the Administrator role and 16 hours for other users. These data can be specified during the development of the Technical specification and reflected in the Technical specification.
* Start-up works.

### Requirements for functional testing

Acceptance tests are carried out in accordance with the requirements of the document "Test program and methodology", which provide for verification of the implementation of the implemented functions of the SWPs.

The test results are drawn up in a protocol of the relevant tests signed by the representatives of the Beneficiary with the participation of the Supplier, the Technical Administrator and the Beneficiary, the test report must be attached to the test protocol.

### Requirements for penetration testing of SWPs

Before transferring the results of the work on creating SWPs to the Beneficiary, the developed SWPs must be tested by penetration and load testing by the Beneficiary in order to identify critical and high information security risks. The Supplier must notify the Beneficiary that the system is ready for testing, after which the Beneficiary organizes and conducts testing within 2 weeks.

In the event of fixing critical and high risks during the penetration testing process, the Supplier must ensure their elimination as soon as possible and report on readiness for re-testing.

The SWPs cannot be accepted by the Beneficiary until all critical and high information security risks have been corrected and verified.

### Acceptance procedure

The results of the provision of services are accepted by the Beneficiary commission.

Representatives of the Supplier are involved in the acceptance of the provided services.

Property, including exclusive, intellectual property rights to the Software product "Information exchange module", including those provided for by the Civil Code of Ukraine, the Law of Ukraine "On Copyright and Related Rights", as well as other legislation of Ukraine and international regulatory legal acts, from the moment of development (creation, modernization) are transferred to SJA on the basis of the relevant agreement on the transfer of property rights to the Software product "Information exchange module".

Property, including exclusive, intellectual property rights to the Software product "Information collection module", including those provided for by the Civil Code of Ukraine, the Law of Ukraine "On Copyright and Related Rights", as well as other legislation of Ukraine and international regulatory legal acts, from the moment of development (creation, modernization) are transferred to HQCJ on the basis of the relevant agreement on the transfer of property rights to the Software product "Information collection module".

### Requirements for support by the Supplier

SWPs users should be provided with all necessary contact information and instructions regarding assistance in case of SWPs malfunctions.

SWPs administrators should have access to effective means of registering complaints from SWPs service recipients, scheduling tasks, providing information on problem-solving methods, etc. (help desk, knowledge base).

The problem-solving components and knowledge base should be completed and accumulated from the SWPs testing phase. The knowledge base should be prepared during the SWPs pilot operation phase so that it can be used by users and administrators to solve the most common problems.

### Requirements for personnel training

The Supplier must provide training for SWPs administrators and users on the developed SWPs.

Number of personnel for training:

* administration and operation support: at least 2 (two) professional IT employees of the Beneficiary and/or Technical Administrator;
* SWPs users: at least 20 (twenty) employees of the Beneficiary and/or Technical Administrator.

Additional training requirements are specified in clause 5.2.1.

The cost of training must be included in the Supplier's price offer.

## Requirements for warranty support

The object of warranty service shall be the SWPs software implemented in accordance with the terms of the contract and the approved Technical specification.

Warranty service of SWPs is provided after the introduction of SWPs into industrial operation.

Warranty service shall include:

* free correction of errors in the SWPs software;
* free services for responding to incidents related to defects in the SWPs software;
* elimination of discrepancies between the SWPs software and the approved Technical Specifications, errors and other malfunctions (a SW malfunction will be considered a situation when users cannot perform certain actions related to the SWPs functions, except for situations where such failure is a consequence of incorrect operation of the SWPs hardware or communication channels);
* other guarantees provided for by legislative and regulatory acts of Ukraine.

SWPs warranty services apply to the entire list of software provided by the Supplier, including DBMS.

SWPs software must be functional, reliable and quickly restored after error correction. All Supplier actions during the warranty service phase must be performed in accordance with the procedure agreed with the Beneficiary and lead to ensuring the restoration of the Beneficiary's business processes to implement the functionality based on the requirements presented in this document.

Warranty support does not apply to the following cases:

* improper operation or maintenance of the SWPs by the Beneficiary and/or the Technical Administrator (improper operation is considered to be a violation of the conditions and rules for operating the SWPs, which are described in the operational documentation);
* use of elements in the SWPs not supplied by the Supplier, unless the requirements specify a different procedure, or unless the Supplier approves a different procedure;
* if the SWPs or their components (program code and/or database structure, hardware, communication channels, etc.) are modified in any way by the Beneficiary or third parties without the written consent of the Supplier, or the conditions for operating the SWPs, specified in the Operational Documentation, are violated.

All SW SWPs operation errors are classified as:

* critical error – if a violation or problem is detected that prevents 10 percent of users from using the required functions of the SWPs and no other alternative implementation of this function is known;
* non-critical error or violation – if a violation or problem is detected that prevents the user from performing the required functions, but there is an alternative implementation of the function, or if a violation is detected that causes difficulties when using the SW SWPs, but this does not affect the operation of the system functions of the SWPs, or if the error has a minor impact on less than 10 percent of users of the SW SWPs.

The Supplier must analyze the violation or error and determine a way to eliminate it no later than 12 hours after registration in the error log, regardless of the type of registered error or violation.

The deadlines for eliminating errors or violations are agreed with the Beneficiary, but cannot be more than:

* 24 hours for critical;
* 14 days for non-critical.

The calculation of the time period begins from the moment of notification of the Supplier about the violation or error / critical error.

Information on corrected errors or violations is updated and submitted in the form of reports every 3 months.

Beneficiary may, but is not obliged to, purchase additional working hours of Supplier services for additional work on technical maintenance and development of SW SWPs. The need to purchase this work may arise as a result of:

* • changes in the legal environment governing the Beneficiary's activities;
* • other external risk factors that were not foreseen during the design and implementation of the SW SWPs;
* • lack of specialists at the Beneficiary with the necessary qualifications to configure and maintain the operability of the SW SWPs.

Additional services to support and develop SWPs may include:

* implementation of functionality not provided for by the requirements for SW SWPs, i.e. modification of SW according to additional functionality needs. In each individual case, before starting work, the Supplier must consider in detail and agree with the Beneficiary a description of the planned development of additional modifications, time costs with their justification and the deadline for implementation;
* providing support in restoring the functionality of the operating system, for example, after disruptions in the operation of the database or its individual components, when the nature of the disruptions is not the subject of service maintenance.

The Beneficiary must purchase additional support and development services for SWPs as a separate service from the main contract.

When implementing additional support and development services for SW SWPs, functionality, reliability and rapid recovery of SWPs after violations must be maintained. All actions of the Supplier to implement SWPs when providing additional support and development services for SWPs must be performed in accordance with the procedure agreed with the Beneficiary.

If problems or errors in SWPs are caused by the provision of additional support and development services for SWPs described in this section, their removal and correction must be carried out as a warranty.

# Conclusions

The creation of SWPs is an effective, efficient and essentially necessary means of achieving the goals set by the Law of Ukraine “On the Judiciary and the Status of Judges”, the Law of Ukraine “On the Prevention of Corruption”, strategic and program documents of the Cabinet of Ministers of Ukraine, international documents on the prevention of corruption in Ukraine.

Improving the quality of automated work processes is achieved through the maximum implementation of paperless technology at all stages of information formation and analysis, acceleration of document flow, use of electronic identification with mandatory use of QES, application of effective control over all technological operations, application of more modern technical means, unification of document forms and concentration of message exchange between different systems (external and internal) through a single point.

# Annexes

## Annex 1. Layout of the information card for the subject of the inspection

Section 1. Information about the subject

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Last name | First name | Patronymic (if available) | Individual tax number (if available) | Date of birth |
|  |  |  |  |  |

Section 2. Information about the subject’s family members and close relatives

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Relationship with Subject | Last name | First name | Patronymic (if available) | Individual tax number (if available) | Date of birth |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Section 3. Real estate

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Full name of the subject or family member | Object type | Date of right acquisition | Cost at the date of acquisition | …  Other key fields  … | View the original response | View a visual representation |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Section 4. Vehicles

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Full name of the subject or family member | Object type | Date of right acquisition | Cost at the date of acquisition | …  Other key fields  … | View the original response | View a visual representation |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Section X. “Name of external source of information”

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Full name of the subject or family member | Object type | …  Other key fields  … | View the original response | View a visual representation |
|  |  |  |  |  |
|  |  |  |  |  |

## Annex 2. List of external sources of information

As part of the project implementation, the Supplier must ensure the implementation of information interaction with the above ESoI regarding the provision and receipt of data, with the owners of which, at the time of completion of the Technical specification preparation stage, relevant documents (contracts, exchange protocols, etc.) will be signed, establishing legal relations regarding information interaction.

|  |  |  |
| --- | --- | --- |
| № | Registry name (ESoI) | Owner / Technical Administrator |
| 1 | State register of civil status acts of citizens | Ministry of Justice, NAIS |
| 2 | State register of property rights to immovable property | Ministry of Justice, NAIS |
| 3 | State register of movable property encumbrances | Ministry of Justice, NAIS |
| 4 | Unified state register of vehicles | МВС |
| 5 | Unified register of powers of attorney | Ministry of Justice, NAIS |
| 6 | The unified state register of legal entities, natural persons - entrepreneurs and public formations | Ministry of Justice, NAIS |
| 7 | Unified state register of court decisions | SJA |
| 8 | State register of natural persons - taxpayers | State tax service of Ukraine |
| 9 | Integrated interdepartmental automated information exchange system on the control of persons, vehicles and cargo crossing the state border, "ARKAN" | Administration of the state border guard service of Ukraine |
| 10 | The state land cadastre | State service of Ukraine for geodesy, cartography and cadastre |
| 11 | Information databases of the national securities and stock market commission | National securities and stock market commission about the securities market |

## Annex 3. Stage implementation schedule

**Estimated schedule for the implementation of the stages of the SWPs life cycle**

|  |  |  |
| --- | --- | --- |
| **Stage of work** | **Stage result** | **Deadline** |
| 1. Development of the technical specification for the SWPs | Technical specification - approved | No later than 2 months after signing the Agreement |
| 1. SWPs software development | Software product - developed  Software product in sufficient volume for experimental testing - delivered | No later than 6 months after signing the Agreement |
| 1. Introduction of SWPs into experimental operation, including | Testing of the SWPs software in the scope of preliminary tests - conducted.  User training - conducted.  Experimental operation of SWPs - conducted | No later than 7 months after signing the Agreement |
| 1. SWPs warranty service | Provision of warranty services for SWPs – 12 months | Within 12 months of completing Stage 3 |

It is allowed to carry out individual stages of the project before the completion of previous stages, to carry out project stages in parallel in time, and to include new stages of the project, taking into account the specifics of the SWPs being built.

## Annex 4. Requirements for potential suppliers

Considering the requirements for SWPs and the scope of work to create them, it is recommended to establish the following qualification requirements for development organizations that need to be involved in the creation of SWPs, according to the following criteria:

**Financial capacity**

Over the past 3 (three) years, the bidder must have an average annual turnover of not less than one hundred thousand (100,000) US dollars or the equivalent of this amount in other currencies at the cross rate of the National Bank of Ukraine at the end of the relevant year.

**Experience and technical ability**

Over the past 5 (five) years, the bidder must have successfully completed at least two (2) contracts for:

* development, supply, implementation, provision of warranty/post-warranty service and/or technical support for the operation of similar information systems (automated information systems that have similar functional and technical characteristics to the SWPs being created);
* development and implementation, or provision of technical support for the operation of automated data exchange between state registers and information databases.

**Personnel**

The bidder must have the following qualified staff:

* Project Manager;
* Architect/Software Development Team Leader;
* Analyst;
* Database Engineer;
* Software Developer (2 people);
* DevOps;
* Documentation Specialist;
* System Administrator;
* Tester.

**Availability of equipment and material and technical base**

The bidder must own or have access to a material and technical base that will fully allow it to independently implement the development of SWPs software without using the Beneficiary infrastructure, namely: the availability of appropriate computing capacity (servers, computers and other automation tools), telecommunications (switching) capacity and licensed software.