Decision-making in the recommendation system of personnel security of the company

A Shelupanov, M Nemirovich-Danchenko and S Glukhareva
Tomsk State University of Control Systems and Radioelectronics, Russia, Tomsk
E-mail: samantases@mail.ru

Abstract. The paper provides an assessment of personal's reliability in the personnel security system of a company. The analysis of existing solutions in various industries is carried out. The stages of assessment and levels of reliability are shown.

1. Introduction
Over the past five years, the number and scale of economic crimes within the company has grown significantly. Resource theft, industrial espionage, disclosure of trade secrets cause immense harm to the company's economy. Along with external destabilizing factors, any company bears internal risks associated with the actions of its personals. To reduce these risks at the stage of personnel assessment and monitoring the state of personals, various assessment methods are used to assess whether or not the personnel have the necessary competencies for work, the most suitable for a specific position, individual traits and socio-psychological qualities of a person or, on the contrary, dangerous psychological properties and facts of activity. In the digital age, HR departments use software packages to evaluate personnel assessment and make decisions.

Many global companies use various methods of personnel assessment, for example, Management by objectives, Performance management (PM), Assessment Center, peer review, etc. These methods have formed the basis of digital solutions of many companies: SaaS, TalentQ, etc.

Currently, great importance is given to companies that have critical information infrastructure (CII) facilities. It is natural that experts consider the effective provision of personnel security to be one of the most priority areas that ensure the stability of development and competitive advantage for companies, and on the scale of the economic system of the state as a whole [1].

Under the personnel security we mean "the system of a company associated with the effective work of personnel and the functioning of the organization (company) in safety conditions and aimed at the development of the organization itself as a whole, and each personal individually" [2].

2. Software package «Personnel security system of the company» to CII
The personnel security system CII of a company is a software package consisting of three modules: questioning, testing and cases. Based on the results of passing each module, the level of reliability is determined. It is a system of human resources personnel for decision making.

The personnel assessment methodology in this system is based on the compilation of a competence profile for each specific position [3]. The structure of competencies includes the following main blocks of competencies: personal, professional, corporate, security, specialty, social, socio-psychological, etc.
The system is a website and a client (desktop) application "Expert". The server part of the "Company Personnel Security system" is a physical dedicated server running the "Microsoft Windows Server" operating system. A strictly limited number of people have access to the server.

The "MySQL" DBMS acts as a database. It stores all the data of users who register, fill in a questionnaire and are tested on the site, as well as information about users (login, access rights, etc.) of the client application. Communication of the server application with the database is performed through SQL queries.

Node.js, an asynchronous event-driven JavaScript environment designed for creating scalable network applications, acts as a Web application of the personnel security recommendation system. A web application consists of a client (frontend) and a server (backend) parts.

The client part of the Web application is implemented in the form of a website where users can pass questionnaires and testing after registration. To access the site, users use their workplace.

The server part of the Web application is responsible for processing all requests, including automated processing of test results and questionnaires. In addition, the server application provides an API for the client application, with which you can receive and send data.

Electron acts as the client part of the system. This framework is used to develop cross-platform applications using Node.js and Chromium rendering libraries, which allows using web technologies (HTML, CSS and JavaScript) for development. The "Expert" client application has a separate list of users (experts and administrators) that is not associated with the list of site users (candidates). Figure 1 shows the scheme of the system functioning.

![Diagram of the system functioning](image)

**Figure 1.** The scheme of the system functioning

Frontend communicates with the backend using HTTP requests over a secure channel (HTTPS):
- GET requests are designed to receive data from the server;
- POST requests are used to send data to the server and receive a response.
Upon receipt of any request or response, the received data is checked, both the structure of the received data and the data type are checked. Thus, if a request requires information about a certain user and contains an integer value of the identifier (ID), then if there is other data or a value of a different type, the request will be rejected and recorded in the error log.

The remote client (the desktop application "Expert") must first pass authorization to receive any information from the server. After successful verification of the authentication information (login and password), a unique GWT (Json Web Token) is created for the client and sent in response to the authorization request.

When registering on the site, you must specify your email address (login) and password, as well as confirm your consent to the processing of personal data.

After registration, users can go through the questionnaire stage, in which it is necessary to answer a number of questions, both open and closed.

As soon as the site user has filled in the questionnaire, special algorithms automatically process the results and the level of reliability is determined from 0 to 1. Based on this score, the first screening of candidates (with a low score) takes place. For those participants who did not score a passing score, an explanation is formed, which displays the main criteria that influenced the receipt of a low score. Users with a passing score are allowed to the testing stage.

The system itself determines which tests need to be passed, based on the competence profile. The personal's potential is also determined in the system.

Each test contains a set of questions in a text or graphical representation with the choice of an answer (one or more from the list) or entering it manually in the appropriate fields (for example, entering a missing word, letter or a certain sequence of characters).

Some questions are limited in time for memorization (pictures, sequences of words or numbers, and so on). Any test is available to the user only once (only the expert can activate the repeated passage) and closes at the beginning of the passage.

All tests are limited in time (from two minutes to an hour or more). As soon as the user runs out of time, only the responses that were selected will be sent to the server. Depending on the methodology, blank tests will be processed either partially or rejected (a minimum score is set). As in the case of the questionnaire, each test is evaluated with a score from 0 to 1. After passing all the tests by a specific user, a score from 0 to 1 is set for him (the initial level of reliability is determined), based on the points for the questionnaire and testing stage. In case of receiving a low score, a report is generated, which indicates the most significant competencies of the candidate that he needs to master. Upon receiving a passing score, the user is allowed to the next stages.

The grade of assessment is divided into "high", "medium" and "low" level of reliability. The “high” level coefficient is in the range from 0.75 to 1, “medium” from 0.45 to 0.74, and “low” from 0 to 0.44, respectively. To advance to the next stage, you must have a reliability level above 0.44. Within the framework of the recommendation system, a personal with a reliability level of at least 0.45 is considered for further work. A person with a "average" level of reliability is not allowed to go through further stages. A person with an "average" level of reliability can be hired, subject to further work on his "weak" sides, in order to increase his level of reliability. A person with a "high" level of reliability will definitely advance to the next stage. To ensure personnel security, a person needs an average and high level of reliability. The person who received -2 did not meet the time limit when passing the test. A -1 means that the person did not pass the test to the end.

The client application called "Expert" is designed for an expert. With this application, it is possible to see the registered users of the system.

The main page shows a list of users and their basic information (for example, mail, gender, age, and the result of processing the questionnaire stage).

By selecting the profile of any of the users in the client application, the profile page of this user opens. On the page, user can not only study the result obtained at any stage, but also see the answer options, in the case of testing, or a completed questionnaire.
The client application allows managing user profiles for drawing up an individual test plan (adding methods to the basic set), reactivating tests, and so on. In addition to the expert, an administrator has an access to the application and can manage the accounts (create, reset the password, change access rights) of experts.

3. Decision-making in the personnel security system of the company

Figure 2 shows one of intermediate results of the work of the personnel security system of the company. The general light gray background in the drawing is the absence of an answer. (For example, some test could simply not be planned for some category of personal). The entire legend is shown in the graphic card allows one to see the whole picture. Therefore, poor preparation for testing will lead to an increase in black and dark gray areas, low competence of a group of personnel will give significant red spots, etc.

Figure 2. Graphic map of the intermediate test result

Guided by the legend given below and based on the map of Figure 2, the decision-maker (PLR) can formulate both tactical and strategic conclusions (including recommendations).

Based on the data obtained, individual plans for the development of personnel who have received an average level of reliability (0.45-0.74) and a career plan for the development of personnel who have scored from 0.75 to 1, that is, a high level of reliability, can be drawn up.

The following measures can also be recommended: creating favorable working conditions suitable for the successful development of personnel, financial incentives for personnel, assistance in adapting personnel, holding master classes, conferences, trainings, etc.

Thus, the practical application of these recommendations will significantly increase the personnel security of the company, minimize the risks associated with personnel, and the implementation of individual and career development plans will improve both personal, professional and behavioral competencies, as well as security and future competencies.
4. Conclusions
The software package allows significantly reducing the cost of the assessment procedure by excluding from the process the personnel involved in personnel management. Another significant advantage is the ability to undergo an assessment remotely, which is especially important in the modern conditions of a pandemic and remote work.

Thus, the basis of personnel security is the personnel of company, namely, competent and conscientious employees with a high level of reliability. Evaluation according to this system is necessary, especially for those who work at CII facilities.

References
[1] Dukhnovsky S V 2019 Personnel safety of the organization: textbook and workshop for the academic baccalaureate (M.: Yurayt) 245 p
[2] Glukhareva S V 2017 Methods of recruiting personnel for positions related to the processing of confidential information. Security of the information space - 2017: XVI All-Russian scientific-practical conference of students, graduate students, young scientists. Yekaterinburg, December 12, 2017. - Yekaterinburg: Ural Publishing House. University, 2018 154-158
[3] Glukhareva S V, Shelupanov A A, Mareeva E V, Abrosimova M E, Eremenko A S and Maltsev V E 2019 Certificate of registration of the computer program RU 2019616940, 05/30/2019. The personnel security system of the company. Application No. 201961601