Laboratory Work – 2

1. Risk: Lack of clarity of requirements:

* Description: Lack of a clear mechanism for determining the requirements for user accounts (jobseekers, employers), which can lead to problems in the registration and authentication process.
* Importance: 4 (important to prevent problems in the initial stage of use)
* Difficulty: 3 (requires more clarity in documentation)
* Mitigation strategy methods:

1. Develop detailed registration scenarios for each type of user.
2. Conduct testing of enrollment scenarios with users to identify potential issues.

* Considered: Yes.

1. Risk: Improper dependency management.

* Description: Lack of integration between different components of the system, such as between the job search system and the application process, which can lead to unexpected errors.
* Importance: 4 (important to ensure the consistent and effective functioning of the system)
* Difficulty: 3 (requires more thorough definition of dependencies)
* Mitigation strategy methods:

1. Development of clear interfaces between the different components of the system.
2. Regular testing of processes that depend on each other.

* Considered: Yes.

1. Risk: Ineffective technology management.

* Description: Potential problems with the operation of payment systems or errors in the mobile application may cause failures that affect the usability of the system.
* Importance: 4 (Critical for Uptime)
* Difficulty: 3 (more thorough testing and updating is needed)
* Mitigation strategy methods:

1. Implementation of a monitoring system and periodic updating of technological elements.
2. Conducting training of personnel on safe and effective methods of using technology.

* Considered: Yes.

1. Risk: Poor security.

* Description: The lack of reliable protection makes the system vulnerable to web attacks such as SQL injections, XSS, and others, which can lead to the leakage of confidential information and loss of user trust.
* Importance: 5 (critical as unsafe practices can lead to leakage of confidential information and loss of user trust)
* Difficulty: 4 (requires high technical expertise and implementation of additional security tools)
* Mitigation strategy methods:

1. Implement a robust Web Application Firewall (WAF) to filter malicious traffic and prevent attacks.
2. Regularly update and audit the application code to identify and fix potential vulnerabilities.
3. Train staff on safe development practices and ensure compliance with security standards.

* Considered: Yes.

1. Risk: Failure to send a confirmation email when a user registers.

* Description: In case of a trivial server glitch during registration, the user may not receive a confirmation of mail, which creates a risk of missing a potential user and losing trust.
* Severity: 5 (critical, missed users, and loss of trust).
* Difficulty: 2 (technical problem).
* Mitigation strategy methods:

1. Replacement of servers with more productive and stable ones.
2. Ability to resubmit a request for written confirmation.

* Considered: Yes.

1. Risk: Lack of platform administrators and help desk.

* Description: The project will certainly someday serve a lot of traffic, to control it, maintaining a large staff can cost a pretty penny for a young company.
* Importance: 4 (very important from the point of view of the perception of the stakeholders of the parties).
* Difficulty: 3 (finding a reliable CRM service provider).
* Mitigation strategy methods:

1. Traffic monitoring to predict staffing needs.
2. Establishing a long-term partnership with a reliable CRM service provider.
3. Automation of routine tasks through an artificial intelligence bot.

* Considered: Yes.

1. Risk: Users misuse their personal profile and post phishing links.

* Description: Users can abuse their profile by posting phishing links, which directly affects the safety of users' data and devices.
* Severity: 5 (extremely important, affects the security of data and devices).
* Difficulty: 2 (solution from the technical part).
* Mitigation strategy methods:

1. Every time you log in to the service, remind the user that they need to keep their eyes peeled and remind them of possible ill-wishers.
2. Ability to check links before publication through the CRM system.

* Considered: Yes.

1. Risk: Mess among messages/requests to the platform administrator.

* Summary: Confusion in various requests can slow down processing and responses, affecting the responsiveness of the service.
* Importance: 4 (affects the responsiveness of the service).
* Difficulty: 1 (easy to solve).
* Mitigation strategy methods:

1. Adding template themes for competent sorting of messages.
2. Redirect to the current administrator in case of urgent need.

* Considered: Yes.

1. Risk: Error management.

* Summary: Confusion when errors occur can slow down the troubleshooting process.
* Importance: 4 (affects the speed of error resolution)
* Difficulty: 2 (difficulty in identifying problems in time)
* Mitigation strategy methods:

1. It's important to create informative error messages in plain language.
2. Implement an error log that will keep a record of the origin of the error and the cause, for more efficient troubleshooting.
3. Appoint individuals who will periodically test different aspects of the system and collect data.

* Considered: Yes.