Common security FAQ

1. **How vulnerabilities are detected and fixed?**
   In applications, the search for vulnerabilities is carried out using regression tests.
   Used to view and analyze documents and source code describing changes in the released product.
   Found vulnerabilities are corrected by IT department specialists.

2. **How frequently are security assessments and scans**?
   Application security assessments are performed whenever code changes that could affect the state of the system.
   Security scans are performed before each distribution is published.
   To achieve this, the company participates in special programs of antivirus manufacturers: Kaspersky company and Avast.
3. **Details of how sensitive data is handled, stored, and transmitted?**
   User data is stored in a protected database that can only be accessed by specialized services.
   User passwords are not stored, stored their hashes only.
   “Salt” is added to the rest of the user data for storage.
   The https and http protocols are used to exchange data between applications and services.
   When using the http protocol, the data is additionally encrypted either with a symmetric encryption or asymmetric encryption is used.
4. **Encryption methods used for data in transit and at rest?**
   Encryption methods AES 256, RSA.
5. **Are firewalls and intrusion detection/prevention systems in use?**
   When applications are running, the integrity of the digital signature is checked while loading the main dlls.