User Manual

The Public security monitoring system "Kipod" is a platform for remote monitoring of objects. The implemented functions include:

- capture automatically abnormal situations, based on the analysis of video and audio streams in accordance with specified rules;
- classify, prioritize, group events coming from remote sites;
- recognize faces and number plates of vehicles in real time, as well as search through the given databases to make a decision about the threat;
- ensure the simultaneous operation of many users in various departments and organizations.

The characteristics and functionality of the System allow the user to monitor state and socially significant objects to ensure public order. Timely detection of abnormal situations helps to quickly make decisions and prevent emergencies.

In addition to improving the effectiveness of security monitoring at sites, the use of the Public safety monitoring system “Kipod” allows operators to process a large amount of data in real time. The system implements an intuitive web-interface, through which the user can:

- form databases for individuals and license plates;
- receive and process events in the alarm monitor mode;
- carry out advanced search for events;
- view live and archive video without installing additional software.

The operation order in the System

Step 1. Loging into the System

The authorized specialist enters the URL of the Public Security Monitoring System "Kipod" in the address bar of the browser. To enter the System, the provided service login and password are used. This user is assigned the role of the System manager (see 4.1. System manager).

Step 2. Changing the service password

The user with the System manager role must change the default password provided for the first login to the System in accordance with the security requirements. To create a new password, it is recommended to follow these rules:

- The password must be at least 8 characters in length.
- The password should consist of numbers and Latin letters in different registers; it is desirable to include in the password other characters available on the keyboard (for example, the symbols??! <> [] {}, etc.).
- The password should not be a dictionary word or a set of characters located next to each other on the keyboard. Ideally, the password should consist of a meaningless set of characters.

Step 3. Performing system settings

The user with the System manager role performs system settings (see 2. Interface), sets the date and time.

Step 4. Adding key users

The user with the System manager role invites users to System and assigns them necessary roles (see 4. User roles). It is recommended to assign the roles of the Camera manager (see 4.2. Camera manager) and the Group manager in the root group (see 4.3. Group manager) so that these users can participate in introducing other users (see 7. Users) and resources to the System.

Step 5. Adding cameras and setting the video analytics

The user with the Camera manager role introduces cameras into the System (see 9. Cameras) and sets the video analytics (see 10. Video analytics). This will automatically create basic entity groups (see 8. Entity groups).

Step 6. Introducing users

The user with the Group manager role creates a tree of user groups (see 6. User groups), populates them with users and assigns them roles.

Step 7. Introducing resources

The user with the Group manager role adds plans (see 11. Plans and facilities) into the System, creates lists of persons (see 12. Persons lists) and lists of numbers (see 13. Number plates lists), assigns them to user groups or users individually for security missions.

Step 8. Checking

The user with the Group manager role checks that the selected user group has access to all the necessary entity groups, cameras, plans, lists of persons and numbers to perform security tasks on the assigned security site, creates an alarm monitor (see 15. Event monitors). The alarm monitor for this user group can also be created by other users of the group who have the necessary permissions (see 5. User permissions).

Step 9. Processing security tasks

The user group can function independently and ensure safety on the entrusted security site.