

# Руководство пользователя

Система мониторинга общественной безопасности «Кипод» представляет собой платформу для удаленного наблюдения за объектами. Реализуемые функции включают в себя:

- автоматически фиксировать нештатные ситуации, на основе анализа видео и аудио потоков в соответствии с заданными правилами;
- классифицировать, приоритизировать, группировать события, поступающие с удаленных объектов;
- распознавать лица и номерные знаки транспортных средств в режиме реального времени, а также производить поиск по указанным базам данных для принятия решения об угрозе;
- обеспечить одновременную работу множества пользователей в различных ведомствах и организациях.

Характеристики и функционал Системы позволяют вести наблюдение за государственными и социально значимыми объектами для обеспечения общественного порядка. Своевременное выявление нештатных ситуаций позволяет оперативно принимать решения и предотвращать чрезвычайные происшествия.

Помимо повышения эффективности мониторинга безопасности на объектах, использование Системы мониторинга общественной безопасности «Кипод» позволяет операторам обрабатывать большой объем данных в режиме реального времени. В Системе реализован интуитивно понятный веб-интерфейс, с помощью которого пользователь может:

- формировать базы данных для лиц и номерных знаков;
- получать и обрабатывать события в режиме тревожного монитора;
- осуществлять расширенный поиск событий;
- просматривать живое и архивное видео без установки дополнительно программного обеспечения.

# Порядок работы в Системе

## Шаг 1. Вход в Систему

Уполномоченный специалист вводит в адресной строке браузера URL-адрес Системы мониторинга общественной безопасности «Кипод». Для входа в Систему используется предоставляемый служебный логин и пароль. Этому пользователю назначается роль Администратора системы (см. [раздел 4.1](#)).

## Шаг 2. Изменение служебного пароля

Пользователь с ролью Администратор системы должен изменить предложенный для первого входа в Систему пароль по умолчанию в соответствии с требованиями безопасности. Для создания нового пароля рекомендуется придерживаться следующих правил:

- Длина пароля должна быть не менее 8 символов.
- Пароль должен состоять из цифр и латинских букв в разных регистрах; желательно включать в пароль другие символы, имеющиеся на клавиатуре (например, символы / ? ! < > [ ] { } и т.д.).
- Пароль не должен являться словарным словом или набором символов, находящихся рядом на клавиатуре. В идеале пароль должен состоять из бессмысленного набора символов.

## Шаг 3. Установка системных настроек

Пользователь с ролью Администратор системы производит системные настройки (см. [главу 2](#)), устанавливает дату и время.

## Шаг 4. Добавление ключевых пользователей

Пользователь с ролью Администратор системы приглашает в Систему пользователей и назначает им необходимые роли (см. [главу 4](#)). Рекомендуется назначить в корневой группе Администратора камер (см. [раздел 4.2](#)) и Администратора группы (см. [раздел 4.3](#)) с тем, чтобы эти пользователи могли участвовать в добавлении пользователей (см. [главу 7](#)) и ресурсов в Систему.

## Шаг 5. Добавление камер и настройка видеоналитики

Пользователь с ролью Администратор камер заводит камеры в Систему наблюдения (см. [главу 9](#)) и производит настройку видеоналитики (см. [главу 10](#)). При этом автоматически будут создаваться базовые группы ресурсов (см. [глава 8](#)).

## Шаг 6. Наполнение пользователями

Пользователь с ролью Администратор группы создает дерево групп пользователей (см. [главу 6](#)), наполняет их пользователями и назначаем им необходимые роли.

## Шаг 7. Наполнение ресурсами

Пользователь с ролью Администратор группы добавляет в Систему планы (см. [главу 11](#)), создает списки лиц (см. [главу 12](#)) и списки номеров (см. [главу 13](#)), назначает их группам пользователей или пользователям индивидуально для решения задач безопасности.

## Шаг 8. Проверка

Пользователь с ролью Администратор группы проверяет, что выбранная группа пользователей имеет доступ ко всем необходимым группам ресурсов, камерам, планам, спискам лиц и спискам номеров для выполнения задач безопасности на закрепленном за ней объектом охраны, создает тревожный монитор (см. [главу 15](#)). Создание тревожного монитора для этой группы пользователей могут произвести и другие пользователи группы, имеющие необходимые права (см. [главу 5](#)).

## Шаг 9. Решение задач безопасности

Группа пользователей может функционировать самостоятельно и обеспечивать безопасности на закрепленном за ней объектом охраны