# Проект автоматизированной системы «Учёт криминогенной ситуации в городе» (актуализированная версия)

## Цель проекта

Создание автоматизированной системы информационной поддержки правоохранительных органов и городской администрации для учёта, анализа и прогнозирования криминогенной обстановки, включая киберпреступления.

## Назначение системы

Система предназначена для: - регистрации и хранения информации о правонарушениях (включая киберинциденты); - учёта мест совершения преступлений и их географической локализации; - ведения данных о фигурантах, сотрудниках, мерах реагирования и результатах расследования; - анализа статистики, выявления криминальных тенденций и «горячих точек» на карте города; - формирования аналитических отчётов для руководства и городской администрации.

## Основные требования к системе

* Учёт всех категорий правонарушений: административные, уголовные, экономические, киберпреступления и др.
* Возможность фиксации даты и времени (или диапазона) совершения инцидента.
* Привязка к точным координатам и типам территорий.
* Возможность привязки к нескольким фигурантам и сотрудникам.
* Поддержка статусов расследования и истории их изменений.
* Учёт мер реагирования и результатов расследований.
* Поддержка аналитических запросов и генерации отчётов.
* Обеспечение безопасности и защиты персональных данных.

## Сущности предметной области

### 1. Правонарушение (Incident)

* Уникальный идентификатор (номер дела/протокола);
* Категория правонарушения (уголовное, административное, экономическое, кибер и др.);
* Статья УК/КоАП;
* Дата и время (или диапазон) совершения;
* Описание инцидента;
* Статус (зарегистрировано, расследуется, раскрыто, передано в суд, закрыто);
* Дата регистрации и сотрудник, принявший сообщение;
* Дата закрытия дела;
* Признак киберпреступления и цифровые атрибуты (IP, MAC, хэши файлов, URL, логи и др.);
* Метаданные (в формате JSONB).

### 2. Место совершения (Location)

* Уникальный идентификатор;
* Адрес;
* Координаты (широта, долгота);
* Тип территории (двор, парк, улица, общественное заведение, сеть и др.);
* История происшествий по данному адресу.

### 3. Фигурант (Person)

* Уникальный идентификатор;
* ФИО;
* Тип участия (подозреваемый, потерпевший, свидетель);
* Дата рождения;
* Адрес проживания;
* Контактные данные;
* Судимости и привлечения к ответственности;
* Признак чувствительных данных.

### 4. Сотрудник (Employee)

* Табельный номер (уникальный идентификатор);
* ФИО;
* Звание;
* Должность;
* Подразделение;
* Контактные данные.

### 5. Мера реагирования (ResponseAction)

* Уникальный идентификатор;
* Правонарушение (ссылка);
* Тип меры (задержание, административный арест, возбуждение дела, выезд, конфискация и др.);
* Исполнитель (сотрудник);
* Дата и время применения;
* Подробности.

### 6. История статусов (StatusHistory)

* Уникальный идентификатор записи;
* Правонарушение (ссылка);
* Исходный статус;
* Новый статус;
* Изменивший сотрудник;
* Дата и время изменения;
* Комментарий.

### 7. Диспетчерская запись (DispatchRecord)

* Уникальный идентификатор;
* Источник (телефон, интернет, мобильное приложение);
* Время получения сообщения;
* Контакт заявителя;
* Краткое описание происшествия;
* Сотрудник-диспетчер;
* Ссылка на связанное правонарушение.

## Взаимосвязи и ограничения

* Одно правонарушение совершается в одном или нескольких местах.
* Одно место может быть связано с множеством правонарушений.
* Один фигурант может участвовать в множестве дел в разных ролях.
* Несколько сотрудников могут участвовать в расследовании одного дела.
* Каждое правонарушение должно быть связано минимум с одним местом.
* Для киберпреступлений обязательно наличие технических данных (IP, URL, логи, хэши).

## Пользователи системы и их функции

### 1. Диспетчеры

* Регистрация входящих сообщений;
* Создание карточек инцидентов и первичных данных;
* Передача дел оперативникам.

### 2. Оперативные сотрудники и следователи

* Внесение данных о правонарушениях, фигурантах, местах;
* Привязка мер реагирования;
* Отслеживание статусов расследования;
* Формирование отчётных документов.

### 3. Аналитики и руководство

* Просмотр сводной статистики;
* Анализ данных по районам, времени, типам правонарушений;
* Определение «горячих точек»;
* Формирование отчётов об эффективности подразделений и динамике преступности.

## Форматы отчётов

* Сводная таблица: Район города — строки, Тип правонарушения — столбцы, Количество инцидентов — значения;
* Динамика количества правонарушений по месяцам/кварталам;
* Рейтинг районов и улиц по числу инцидентов;
* Процент раскрываемости по категориям;
* Возрастная и социальная статистика фигурантов;
* Отчёты по киберпреступлениям (вид атаки, источник, метод, результат).

## Технические требования к реализации

* СУБД: PostgreSQL (с расширением PostGIS для работы с геоданными);
* Все идентификаторы — UUID;
* Индексация по полям даты, статуса, категории и координатам;
* Хранение файлов (доказательств, отчётов) в защищённом объектном хранилище;
* Использование JSONB для хранения переменных атрибутов (например, метаданных киберинцидентов);
* Поддержка ролевой модели (RBAC) и разграничение прав пользователей;
* Журналирование всех изменений и обращений к данным;
* Шифрование персональных данных и логирование доступа.

## Безопасность и конфиденциальность

* Хранение и обработка ПДн в соответствии с законодательством;
* Аудит всех действий пользователей;
* Маскирование персональных данных при аналитических выгрузках;
* Контроль доступа к файлам и протоколам расследований;
* Регулярное резервное копирование и репликация базы данных.

## Итог

Автоматизированная система «Учёт криминогенной ситуации» должна обеспечить: - централизованное хранение и доступ к информации о правонарушениях, включая киберпреступления; - эффективное взаимодействие диспетчеров, оперативников, следователей и аналитиков; - возможность комплексного анализа, прогнозирования и визуализации криминальной активности; - высокий уровень защищённости данных и прозрачности работы системы.