**I. Определение негативных последствий от реализации угроз**

1. **Для автоматизированной системы управления транспортом:**
   1. **Нарушение работы светофоров и GPS-трекинга → ДТП, задержки транспорта (Н.1, Н.44).**
   2. **Утечка данных о маршрутах и расписаниях → Манипуляции с транспортом (Н.30, Н.7).**
   3. **Отказ системы → Остановка движения (Н.6, Н.26).**
2. **Для электронной приемной граждан:**
   1. **Утечка персональных данных → Нарушение конфиденциальности (Н.7, Н.8).**
   2. **DDoS-атака → Невозможность подачи обращений (Н.36, Н.25).**
   3. **Подмена информации → Распространение ложных данных (Н.43).**

**II. Инвентаризация систем и объектов воздействия**

**Объекты воздействия:**

1. **О.2 — Сервер управления транспортом (хранение данных о маршрутах, светофорах).**
2. **О.5 — Модуль IoT (датчики движения, GPS-трекеры).**
3. **О.6 — Маршрутизаторы для связи между системами.**
4. **О.11 — База данных обращений граждан (электронная приемная).**
5. **Од.1 — ПО электронной приемной (веб-интерфейс, CRM).**

**III. Источники угроз**

1. **Внутренние:**
   1. **Сотрудники с избыточными правами (К.4.1.1 — администраторы).**
   2. **Ошибки в настройке оборудования (К.2.4.3 — межсетевой экран).**
2. **Внешние:**
   1. **Хакерские группы (эксплуатация уязвимостей — СП.1.1).**
   2. **Фишинговые атаки на сотрудников (СП.13.4).**
   3. **Природные угрозы (перебои электроснабжения).**

**IV. Оценка возможностей нарушителей**

| **Уровень** | **Описание** | **Пример угрозы** |
| --- | --- | --- |
| **В.1** | **Низкий (скрипт-кидди)** | **Фишинг (СП.13.4), DDoS (СП.14.2).** |
| **В.2** | **Средний (опытные хакеры)** | **SQL-инъекции (СП.22.1), подмена ПО (СП.5.1).** |
| **В.3** | **Высокий (государственные акторы)** | **Атаки на микропрограммы (СП.23.1), туннелирование (СП.11.4).** |

**V. Способы реализации угроз**

1. **Для транспорта:**
   1. **Эксплуатация уязвимостей в ПО светофоров (СП.1.1 → УБИ.8).**
   2. **Подмена данных GPS-трекеров (СП.4.4 → УБИ.4).**
2. **Для приемной:**
   1. **Фишинг сотрудников (СП.13.4 → УБИ.1).**
   2. **SQL-инъекции в базу данных (СП.22.1 → УБИ.2).**

**VI. Оценка актуальности угроз**

| **Угроза** | **Вероятность** | **Ущерб** | **Актуальность** |
| --- | --- | --- | --- |
| **DDoS на приемную** | **Высокая** | **Средний** | **Высокая** |
| **Утечка данных GPS** | **Средняя** | **Высокий** | **Высокая** |
| **Подмена светофоров** | **Низкая** | **Критический** | **Средняя** |

**VII. Сценарии реализации угроз**

1. **Сценарий 1:**
   * **Нарушитель (В.2) использует SQL-инъекцию (СП.22.1) в базе данных приемной → Утечка персональных данных (УБИ.1).**
2. **Сценарий 2:**
   * **Хакерская группа (В.3) внедряет вредоносное ПО в систему управления светофорами (СП.4.10) → Нарушение работы транспорта (УБИ.8).**