**Мы будем рассматривать сеть умных рекламных щитов с точки зрения информационной безопасности, применяя кибер-иммунный подход.**

**1) Постановка задачи**

В условиях современного города необходимо обеспечить бесперебойную и безопасную работу сети умных рекламных щитов и цифровых вывесок, которые управляются централизованно и интегрированы с другими городскими системами. Основная задача — предотвратить кибератаки, такие как подмена контента, DDoS-атаки, внедрение вредоносного ПО, и обеспечить защиту данных при передаче. Важно гарантировать, что сеть щитов будет устойчива к внешним угрозам и несанкционированному доступу.

**2) Цели и предположения безопасности**

**Цели безопасности:**

* **Конфиденциальность**: Защита данных о контенте и управляющих командах от несанкционированного доступа.
* **Целостность**: Гарантия того, что только проверенный и подписанный контент будет отображаться на рекламных щитах.
* **Доступность**: Защита системы от DDoS-атак и обеспечение непрерывной работы даже при сбоях или атаках.
* **Аутентификация**: Только авторизованные операторы могут изменять контент и управлять щитами.
* **Обнаружение вторжений**: Оперативное выявление и блокировка любых попыток вторжения или несанкционированного доступа.

**Предположения:**

* Сеть рекламных щитов подключена к интернету и может быть уязвима для внешних атак.
* Существуют операторы, управляющие сетью через центральный сервер.
* Контент обновляется периодически и передается по защищенным каналам связи.

**3) Архитектура решения**

Архитектура кибериммунного решения включает следующие элементы:

1. **Централизованная система управления** — серверы для управления контентом и состоянием сети щитов.
2. **Рекламные щиты и информационные панели** — автономные устройства, подключенные к сети для получения обновлений.
3. **Сегментация сети** — разные сегменты для управления рекламным контентом, экстренными уведомлениями и городской инфраструктурой.
4. **Шифрование данных** — данные, передаваемые между сервером и щитами, шифруются для защиты от перехвата.
5. **Система мониторинга и обнаружения вторжений (IDS/IPS)** — для мониторинга активности сети и обнаружения аномалий.
6. **Аутентификация и контроль доступа** — использование многофакторной аутентификации (MFA) для операторов системы.
7. **Защита от DDoS-атак** — балансировка нагрузки и фильтрация трафика.

**4) Алгоритм работы решения**

1. **Получение команды на обновление контента**:
   * Оператор или система управления загружает новый контент для рекламных щитов.
   * Перед отправкой данные шифруются и подписываются цифровой подписью.
2. **Передача данных**:
   * Контент передается через зашифрованный канал на рекламные щиты.
   * Каждый щит проверяет цифровую подпись контента перед отображением.
3. **Обновление щитов**:
   * Щит принимает и расшифровывает данные.
   * После успешной проверки целостности данные обновляются на экране.
4. **Мониторинг сети**:
   * Система IDS/IPS отслеживает поведение сети, выявляет аномалии (например, подозрительную активность или аномальные запросы).
5. **Действия при обнаружении угроз**:
   * При обнаружении угроз система изолирует скомпрометированные узлы, автоматически блокирует вредоносные команды и переключает щиты на автономный режим.

**5) Безопасность (выполнение целей безопасности)**

1. **Конфиденциальность** обеспечивается за счет шифрования данных, передаваемых между сервером и рекламными щитами.
2. **Целостность** обеспечивается проверкой цифровых подписей каждого фрагмента данных перед их отображением.
3. **Доступность** поддерживается благодаря защите от DDoS-атак с использованием фильтрации трафика и балансировки нагрузки.
4. **Аутентификация** осуществляется через многофакторную проверку, предотвращая несанкционированный доступ к системе управления.
5. **Обнаружение вторжений** осуществляется с помощью систем IDS/IPS, которые контролируют активность в сети в реальном времени и блокируют подозрительные действия.

**6) Негативные сценарии и защита от них**

1. **Подмена контента злоумышленником**:
   * **Защита**: Использование цифровых подписей. Только контент, подписанный доверенными источниками, будет отображаться на щитах.
2. **DDoS-атака на серверы управления**:
   * **Защита**: Фильтрация трафика и балансировка нагрузки, чтобы снизить нагрузку на серверы. Резервные сервера обеспечивают отказоустойчивость.
3. **Физический доступ к щитам и попытка взлома**:
   * **Защита**: Защищенные корпуса устройств с датчиками вскрытия. При несанкционированном доступе система автоматически блокирует устройство и отправляет уведомление оператору.
4. **Внедрение вредоносного ПО через уязвимости сети**:
   * **Защита**: Регулярные обновления безопасности и контроль целостности программного обеспечения устройств.

**7) Тестирование**

**Функциональное тестирование:**

* **Тестирование управления контентом**: Проверка работы обновления контента через сервер, отображение и шифрование данных.
* **Проверка автономной работы**: Тестирование работы рекламных щитов в случае потери связи с сервером.
* **Мониторинг работы системы IDS/IPS**: Проверка на способность выявлять и блокировать подозрительные действия.

**Тестирование безопасности:**

* **Пенетрационное тестирование (Pentest)**: Тестирование системы на уязвимости, в том числе попытки взлома, DDoS-атаки, перехват данных.
* **Тестирование шифрования**: Проверка работы шифрования данных и проверки цифровых подписей.
* **Тестирование отказоустойчивости**: Симуляция перегрузки системы, отключение центрального сервера, проверки переключения на резервные узлы.

**8) Заключение**

Кибериммунный подход к информационной безопасности сети умных рекламных щитов обеспечивает высокую устойчивость системы к современным киберугрозам. Сегментация сети, шифрование данных, использование цифровых подписей и систем мониторинга угроз обеспечивают выполнение целей по защите конфиденциальности, целостности и доступности системы. Предусмотрены механизмы для изоляции атакованных узлов и автоматического восстановления работы при сбоях. Этот подход гарантирует, что даже в случае кибератак городская инфраструктура останется безопасной и продолжит функционировать.

**9) Источники данных на которых основывается отчет**

1. **Документы по стандартизации шифрования и цифровых подписей** (например, NIST, ISO 27001).
2. **Отчеты и исследования по кибербезопасности рекламных и информационных систем**.
3. **Методики разработки и тестирования систем обнаружения вторжений (IDS/IPS)**.
4. **Научные публикации по кибериммунным системам и защите критической инфраструктуры**.
5. **Стандарты и руководства по защите IoT-устройств**.