**Анализ нормативно-правовых механизмов блокирования в сети «Интернет» служебной информации ограниченного распространения: структурная модель и порядок взаимодействия правообладателей информации и органов государственной власти**

**Аннотация**

В статье исследуются правовые и организационные механизмы блокирования служебной информации ограниченного распространения (СИОР) в сети Интернет. Основное внимание уделено досудебному и судебному порядку взаимодействия участников процесса, а также структурной модели, включающей правообладателей, Роскомнадзор, операторов связи и судебные органы. На основе анализа законодательства, судебной практики и технических аспектов реализации блокирования систематизированы ключевые этапы процедур, выявлены проблемы коллатерального ущерба, правовой неопределённости критериев СИОР и технологических ограничений. Результаты исследования могут быть использованы для совершенствования правоприменительной практики и разработки технологических решений.

**Ключевые слова**: служебная информация ограниченного распространения, досудебный порядок, судебный контроль, Роскомнадзор, коллатеральный ущерб.

**Введение**

Защита служебной информации ограниченного распространения (СИОР) является важным элементом обеспечения информационной безопасности. Под СИОР понимаются сведения, не отнесённые к государственной тайне, но требующие ограничения доступа в связи с потенциальным ущербом для государственных, коммерческих или общественных интересов в случае их разглашения. Актуальность исследования обусловлена необходимостью баланса между оперативностью блокирования и соблюдением прав субъектов информационных отношений. В работе анализируются процедуры досудебного и судебного порядка блокирования доступа к СИОР, а также структурная модель взаимодействия участников данного процесса.

**Методология**

Исследование основано на следующих методах:

1. **Догматический анализ** нормативных актов, включая Федеральный закон № 149-ФЗ и Постановление Правительства РФ № 1233.
2. **Изучение судебной практики** (анализ решений арбитражных судов).
3. **Структурно-функциональное моделирование** взаимодействия участников процесса блокирования.
4. **Статистический анализ** данных Роскомнадзора и операторов связи.

**Результаты**

**1. Структурная модель взаимодействия правообладателей информации и органов государственной власти**

Модель включает четыре субъекта:

* **Правообладатель СИОР**: осуществляет мониторинг сети, документирование нарушений и инициирование блокирования.
* **Роскомнадзор**: проверяет заявки, координирует блокирование через операторов связи.
* **Операторы связи**: технически реализуют ограничение доступа   
  (IP-адреса, DPI).
* **Судебные органы**: разрешают споры и проводят экспертизы.

**2. Досудебный порядок блокирования доступа к СИОР**

Применяется в экстренных случаях (угроза национальной безопасности, утечка персональных данных). Процедура включает:

1. Подачу заявки правообладателем.
2. Проверку Роскомнадзором в течение 3 рабочих дней.
3. Блокирование ресурса операторами связи в течение 24 часов.

**3. Судебный порядок блокирования доступа к СИОР**

Используется при оспаривании решений или требовании компенсации ущерба. Этапы:

1. Подача иска в арбитражный суд.
2. Проведение технико-правовой экспертизы.
3. Вынесение решения (срок — до 6 месяцев).

**Обсуждение**

**1. Коллатеральный ущерб**

Основная причина — блокирование по IP-адресам, затрагивающее легитимный контент. Так блокирование работы хостинга создает угрозу недоступности сайтов, функционирующих без нарушения законодательства.

**2. Правовая неопределённость критериев СИОР**

Отсутствие четких критериев отнесения сведений к СИОР позволяет госорганам расширительно трактовать статус информации.

**3. Технологические ограничения**

##### а) **Ограничения методов блокирования**

* **Блокирование по IP-адресам**:
  + **Проблема**: Один IP-адрес может обслуживать десятки сайтов, что приводит к массовому коллатеральному ущербу.
* **DPI (Deep Packet Inspection)**:
  + **Суть**: Технология анализа трафика для точного блокирования контента (например, по URL или ключевым словам).
  + **Ограничения**:
    - Высокая стоимость оборудования.
    - Сложность обработки зашифрованного трафика (HTTPS, VPN).
* **IPv6**:
  + **Проблема**: Отсутствие единых стандартов блокирования для IPv6. Большинство операторов используют устаревшие методы, разработанные для IPv4.

##### б) **Ограничения инфраструктуры**

* **CDN (Content Delivery Network)**:
  + **Суть**: Распределенные сети доставки контента (например, Cloudflare, Akamai) усложняют блокирование, так как ресурс может быть размещен на сотнях серверов.
* **Анонимизирующие технологии**:
  + **TOR и VPN**: Позволяют обходить блокировки, делая их неэффективными.

##### в) **Правовые и экономические барьеры**

* **Отсутствие финансирования**: Малые операторы связи не могут позволить себе DPI-оборудование.
* **Юридические риски**: Операторы опасаются судебных исков за избыточные блокировки.

##### г) **Международный опыт**

* **ЕС**: Используется система «upload filters» для платформ, что снижает нагрузку на операторов.
* **Китай**: Применяется комбинация DPI, Great Firewall и цензуры на уровне провайдеров.
* **Проблема для РФ**: Отсутствие аналогов китайской инфраструктуры и европейских правовых механизмов.

**Заключение**

1. Досудебный порядок обеспечивает оперативность, но требует чёткого соблюдения процедур.
2. Судебный порядок гарантирует защиту прав владельцев ресурсов, однако отличается длительностью.
3. Структурная модель взаимодействия выявляет необходимость:
   * Более четкого определения критериев отнесения сведений к СИОР.
   * Внедрения технологий точечного блокирования (URL-фильтрация).

**Список литературы**

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Постановление Правительства РФ № 1233 от 03.11.1994.