Резюме

Тема: Анализ существующих методов управления доступом к интернет-ресурсам и рекомендации по их применению.

Целью исследования был анализ методов, которые интернет-провайдеры и регулирующие органы могут использовать для ограничения доступа к запрещенным ресурсам в Интернете; потенциальной точности этих методов; оценка степени легкости их обхода; а также наличие в арсенале интернет-операторов мер, препятствующих их обходу; выработка рекомендаций по организационным и техническим решениям, необходимым для управления доступом к сайтам, содержащим запрещенную информацию.

В рамках настоящего исследования были проанализированы современные технологии блокирования:

• по IP-адресу

• по DNS

• по URL

• углубленный анализ пакетов (DPI)

Проведенный анализ существующих методов блокирования позволяет сделать следующий вывод:

Наиболее предпочтительным методом блокирования следует признать комбинированное блокирование с предварительным выделением по IP адресам и дальнейшей фильтрацией по URL (IP+URL). Оно может быть рекомендовано как основной метод для решения данной задачи.

Блокирование на основе комбинированного метода **IP+URL** предлагает достаточную точность, чтобы избежать чрезмерного блокирования, оказывает минимальное воздействие на инфраструктуру сети Интернет, не

снижает ее устойчивость в целом и не нарушает работоспособности других сервисов и приложений.

В сегодняшних условиях для большинства интернет-пользователей применения этого метода будет достаточно, и он позволит ограничивать доступ массовых пользователей к блокируемым ресурсам.

В качестве базового метода рекомендуется метод **IP+URL**, а не метод DPI, так как массовое использование DPI несет существенные риски, является спорным с точки зрения соблюдения права на неприкосновенность частной жизни, приводит во многих случаях к ничем некомпенсируемому удорожанию сети, вносит технические ограничения на развитие сети.

DNS-блокирование, возможно, представляло бы собой более простой и менее затратный вариант, но при использовании DNSSEC оно требует сотрудничества с операторами соответствующих авторитативных DNS-серверов, что, в некоторых случаях, обеспечить более сложно, чем содействие со стороны интернет-провайдеров. Кроме того, DNS-блокирование обладает несколько меньшей точностью указания блокируемого ресурса, чем при использовании метода **IP+URL**. Однако, простота и эффективность этого метода позволяют применять его в случае, когда налажено взаимодействие с DNS-операторами соответствующих доменных зон. Инфраструктурное **блокирование по DNS на уровне авторитативных серверов и реестров можно рассматривать как возможное к применению в качестве дополнительного метода блокирования** в настоящее время и в будущем.

Блокирование IP-адресов не является достаточно точным и надежным методом блокирования сайтов, чтобы рассматривать его для применения либо в качестве первичного метода, либо как элемента комбинированного метода. Использование блокирования IP-адресов приводит к значительному избыточному блокированию и ряду негативных последствий. **Использование блокирования по IP не рекомендуется.**

Следует отдавать себе отчет в наличии технических возможностей для обхода всех методов блокирования, которые относительно просты в применении. Разумеется, методы противодействия обходу существуют, но они имеют ограничения, например, в отношении защищенных соединений и доступа через виртуальные частные сети (VPN).

Тот факт, что для операторов веб-сайтов и конечных пользователей технически возможно обойти блокирование, не означает, что на практике они будут это делать повсеместно. Блокирование веб-сайтов, скорее всего, будет сдерживать случайных и непреднамеренных нарушителей и усложнит распространение незаконной информации среди добросовестных пользователей.

Таким образом, блокирование незаконных ресурсов может способствовать общему уменьшению случаев нарушения в сети Интернет, если оно является частью более широкого набора мер по борьбе с нарушениями.