УДК 004.773

АНАЛИЗ СИСТЕМ ФИЛЬТРАЦИИ И БЛОКИРОВКИ СЕТЕВОГО ТРАФИКА В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

М. А. БЫЛКОВ, Е. Е. ИСТРАТОВА
Новосибирский государственный технический университет
Новосибирск, Россия

Подключение к сети Интернет стало неотъемлемой частью современного образования, но, наряду с полезными материалами, пользователи могут столкнуться с нежелательным либо потенциально опасным содержанием. В связи с этим в образовательных организациях используются системы фильтрации контента, которые регулируют доступ к определённым веб-сайтам, группам ресурсов и сетевым службам [1]. Кроме того, ограниченная пропускная способность каналов связи в учебных заведениях делает критически важным контроль за целевым использованием трафика. Несанкционированная активность, такая как просмотр развлекательного видео или использование соцсетей, негативно сказывается на качестве обучения. В связи с этим поиск эффективных инструментов для управления сетевым трафиком и блокировки нежелательных ресурсов является приоритетной задачей для образовательных организаций [2].

Цель работы заключалась в проведении сравнительного анализа распространенных систем фильтрации сетевого трафика для выявления особенностей их применения в образовательной сети.

Согласно литературным источникам, современная система фильтрации сетевого трафика в образовательном учреждении должна решать не только задачу блокировки отдельных адресов, но и осуществлять функции поддержки «черных» и «белых» списков, блокировки вредоносных ресурсов, безопасного поиска и журналирования истории запросов [3]. Реализовать эти функции можно на уровне DNS-запросов либо на интернет-шлюзе с использованием специализированного межсетевого экрана, причем от выбранного способа зависят точность и сложность настройки и требования к оборудованию.

В настоящее время наиболее распространенными программными продуктами для фильтрации и блокировки сетевого трафика являются SkyDNS, UserGate NGFW, Ideco NGFW.

SkyDNS представляет собой облачную систему DNS-фильтрации. Запрос к доменному имени направляется на сервер сервиса, где адрес проверяется по категориям и заданным правилам. Администратор может использовать разрешающие и запрещающие списки и отдельные профили доступа. Такой подход сравнительно просто внедрить на центральном маршрутизаторе или DNS-сервере. Его ограничение связано с тем, что решение в основном принимается по доменному имени без анализа полного URL и содержимого страницы.

UserGate NGFW выполняет фильтрацию непосредственно на сетевом шлюзе. В правилах могут учитываться пользователь, IP-адрес, URL, категория сайта, тип содержимого, время обращения и заданные слова или выражения. Система работает с HTTP и HTTPS, а при необходимости может анализировать расшифрованный защищенный трафик, что позволяет задавать разные политики для учебных аудиторий, преподавателей и других групп, но требует более внимательной настройки правил и контроля журналов.

Ideco NGFW также относится к комплексным сетевым шлюзам. Его контент-фильтр проверяет ресурс по встроенным и пользовательским категориям, после чего применяет разрешающее или запрещающее действие. Для HTTPS без расшифровки доступна фильтрация по домену, а для анализа полного адреса страницы требуется расшифровка трафика. Журнал веб-трафика помогает определить, какое правило сработало, что удобно при разборе ошибочных блокировок.

Таким образом, в результате исследования было установлено, что DNS-фильтрация удобна для быстрого введения единых ограничений на большом числе компьютеров, тогда как решения класса NGFW обеспечивают более детальный контроль и разграничение правил доступа пользователей. При этом полностью полагаться только на автоматическую блокировку нельзя, т. к. базы категорий и состав интернет-ресурсов постоянно меняются. В связи с этим необходимо предусмотреть вариант, при котором настройка, проверка и корректировка доступа ко всем ресурсам образовательного учреждения осуществляются на регулярной основе. Также при выборе системы фильтрации и блокировки сетевого трафика следует учитывать размер сети, количество пользователей и квалификацию администратора. Для небольшой сети может быть достаточно централизованной DNS-фильтрации, а для крупного учебного заведения целесообразно использовать шлюз с категоризацией ресурсов, журналированием и раздельными политиками доступа. Наиболее надежный результат в этом случае обеспечит сочетание технической фильтрации с организационным контролем использования сети Интернет.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. **Бахтеев, Д. В.** Преодоление нелегальной трансграничной передачи персональных данных / Д. В. Бахтеев, А. М. Сосновикова, Е. В. Казенас // Journal of Digital Technologies and Law. – 2024. – № 4. – С. 943–971.

2. **Монгуш, М. К.** Организация безопасного доступа к сети Интернет в образовательных учреждениях / М. К. Монгуш, П. М. Тапышпан // Вестник Тувинского государственного университета. Педагогические науки. – 2016. – № 4. – С. 137–145.

3. **Емельянов, Д. Д.** Фильтрация сетевого контента в образовательных учреждениях / Д. Д. Емельянов // Педагогическое образование в России. – 2018. – № 8. – С. 75–82.