

В школе используется следующая система фильтрации трафика, состоящая из трех компонентов

1 - На уровне провайдера, все ресурсы (сайты) из Реестра запрещенных сайтов блокируется на маршрутизаторе провайдеров предоставляющих доступ к сети "Интернет"

2 - Служба Яндекс.DNS (<https://dns.yandex.ru/>) с включенным фильтром "Семейный" в качестве основного DNS на маршрутизаторе.

3 - Внутренним межсетевым экраном. В качестве средства для организации системы ограничения доступа к сайтам в сети "Интернет" в кампусах используются многофункциональные сетевые UTM-устройства (маршрутизаторы) FortiGate 100D и Fortigate 110C производства компании Fortinet. Подписка на сервисы Fortinet позволяют получать ежедневное обновление нежелательных ресурсов по многим категориям (<https://fortiguard.com/webfilter>) А так же принудительный включенный безопасный поиск в Google.

Алгоритм работы решения:

- На устройство загружается список запрещенных сайтов.
- FortiGate вычисляет IP-адреса перечисленных URL путем DNS-запросов. Результат DNS-запроса сохраняется в течение указанного TTL. По истечению TTL выполняется повторный запрос.
- Если в запросе от пользователя содержится IP-адрес, соответствующий URL адресу из черного списка, «подозрительный» трафик направляется на устройство Fortigate.
- Fortigate сравнивает URL из запроса с загруженным списком запрещенных сайтов.
- При совпадении URL запрос блокируется.
- Обратный трафик из Интернет до абонента доходит по прямому маршруту.

Данная схема не предоставляет возможности блокировать материал без явного адреса (URL). Т.к технически нет возможности полностью блокировать контент по семантике без нарушения доступа к части ресурсов, используемых для обучения, а также анализировать изображения на предмет наличия запрещенного контента.