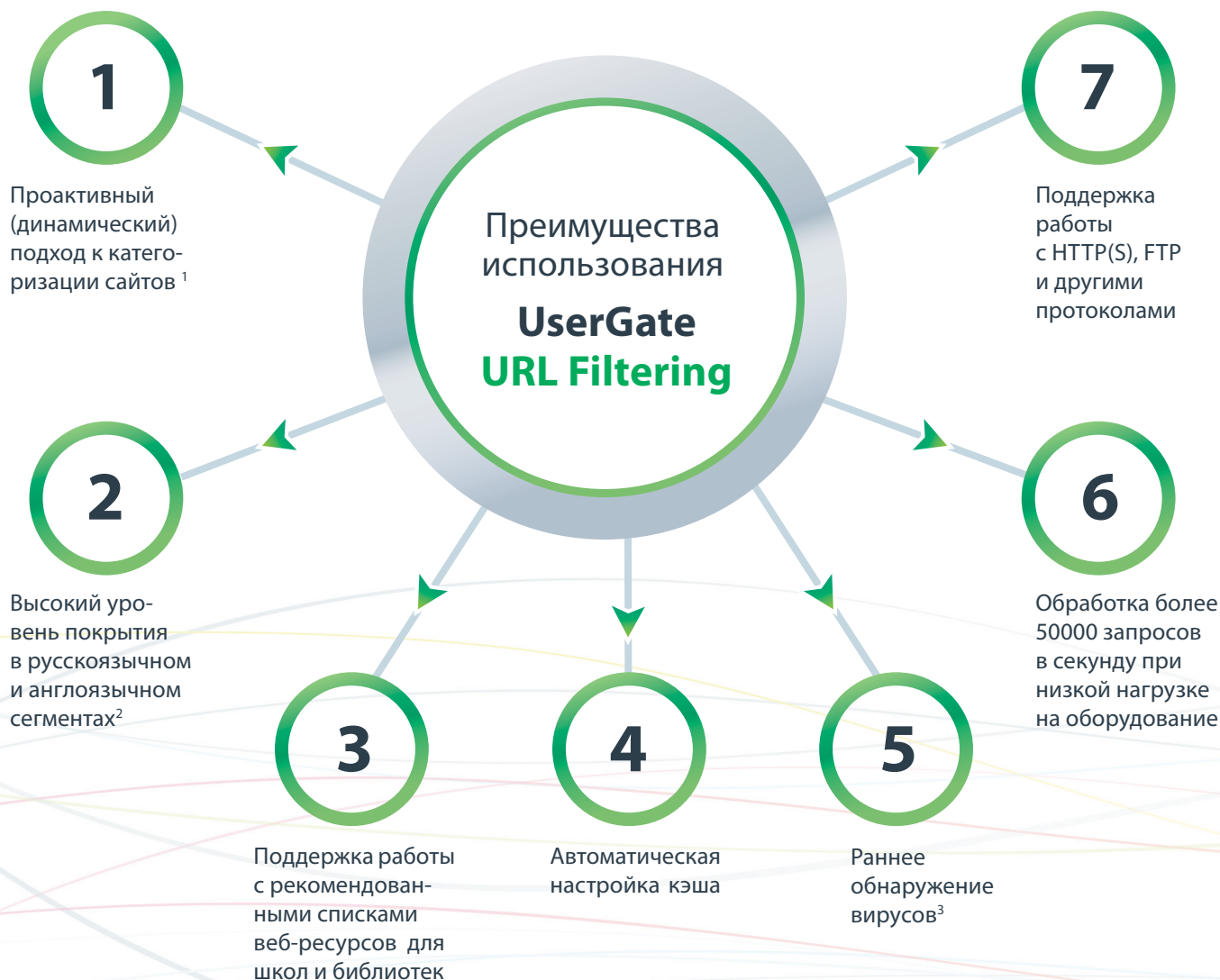


# Технология фильтрации

## UserGate URL filtering

UserGate URL Filtering – технология интернет-фильтрации, основанная на одной из самых больших баз сайтов (более 500 миллионов), для удобства использования разделенной на категории.

Данный набор покрывает практически все виды ресурсов, включая сайты с вредоносными программами, экстремистского и националистического содержания, социальные сети и порталы знакомств.



<sup>1</sup> Большинство средств фильтрации при появлении нового интернет-ресурса относят его к определенной группе и больше не возвращаются к нему. Подобные недостатки систем используются злоумышленниками: контент сайта может быть кардинально изменен, а фильтр будет относить его к старой категории. UserGate URL Filtering использует базу ресурсов, поддерживаемую в самом актуальном состоянии посредством постоянного мониторинга сайтов.

<sup>2</sup> Высокий уровень покрытия в русскоязычном и англоязычном сегментах, подтвержденный результатами независимого тестирования средств родительского контроля на [http://www.anti-malware.ru/parental\\_control\\_tests](http://www.anti-malware.ru/parental_control_tests). Технология адаптирована для работы с ресурсами доменных зон .ru, .рф, .su, .ua, .kz и других, связанных со странами бывшего СССР. UserGate сотрудничает с RU-Center и проводит работу по полной категоризации ресурсов Рунета.

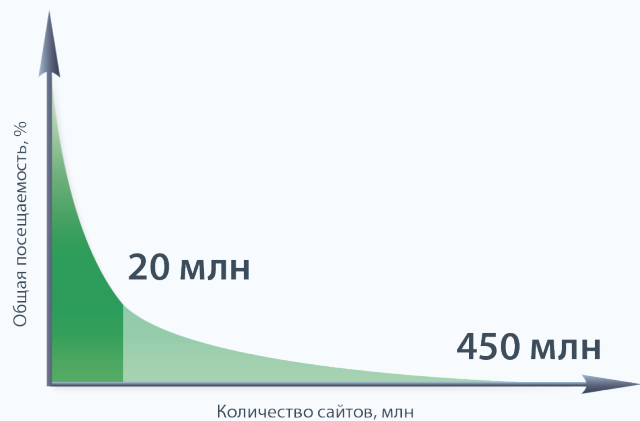
<sup>3</sup> UserGate использует статистический анализ атак и эпидемий на базе данных от сотен серверов по всему миру. Это обеспечивает самое быстрое время реакции на возникновение новых угроз.

Работа модуля фильтрации по категориям сайтов основана на технологии UserGate URL Filtering, в которой используется категоризированная база, содержащая более 500 млн. сайтов. Администратор может запрещать доступ к отдельным сайтам, к категориям сайтов, либо к тем сайтам, адреса которых содержат заданные фрагменты слов. База специально адаптирована для использования русскоязычными пользователями и содержит до 10 миллионов русскоязычных сайтов.

Использование URL-фильтрации обеспечивает безопасность локальной сети за счет ограничения доступа к потенциально вредоносным сайтам.

База UserGate URL Filtering выделяется из массы альтернатив благодаря наличию в базе данных даже тех сайтов, уровень посещаемости которых очень низок. Такие сайты получили общее название "Long Tail", из-за формы графика распределения посещаемости между веб-ресурсами.

Согласно статистическим данным, около 50% мировой посещаемости Интернет-ресурсов приходится на 20 миллионов сайтов, находящихся вверху списка посещаемости. Оставшиеся 50% посещаемости приходятся на группу сайтов объединенных термином Long Tail, которая в десятки раз превышает по количеству первую группу.



Большинство решений по контентной фильтрации, представленных сегодня на рынке, в основном концентрируется на наиболее посещаемых сайтах (20 миллионов сайтов), упуская из виду тот факт, что таким образом охватывается лишь половина от общего количества веб-запросов.

Как следствие, компании, использующие эти решения могут столкнуться с риском заражения локальной сети сетевыми вирусами и червями, поскольку угрозы такого характера одинаково представлены на всех ресурсах, а не только на наиболее посещаемых.

При использовании UserGate URL Filtering высока вероятность того, что практически любой ресурс, который посещает пользователь гарантированно окажется в базе данных в одной из категорий, а следовательно — доступ к такому ресурсу или категории можно будет ограничить.

Из всех решений, доступных сегодня на рынке, только используемая UserGate база насчитывает более 500 миллионов URL-адресов, которая охватывает как наиболее популярные сайты, так и менее посещаемые ресурсы.

Технология UserGate URL Filtering сравнима по принципу работы с облачными антивирусом и анти-спамом, внедренных в продукты UserGate. Интернет-ресурсы, угрожающие безопасности компьютера, обнаруживаются еще до того, как тысячи рабочих станций пострадают от их воздействия.

# Категории сайтов

## Информационная безопасность

Категории сайтов, запрет доступа к которым позволит избежать ряда проблем с информационной безопасностью.

- Анонимайзеры
- Сетевые ошибки
- Криптомайнеры
- Зараженные сайты
- Паркованные домены
- Фишинг и мошенничество
- Ботнеты
- Спам-сайты
- Вредоносное ПО

## Родительский контроль

Группы интернет-ресурсов, не рекомендуемые для посещения детьми.

- Алкоголь и табак
- Социальные сети
- Сайты знакомств
- Религиозные культы
- Половое воспитание
- Пиринговые сети
- Нелегальное ПО
- Нецензурная лексика
- Порнография и насилие
- Преступная деятельность
- Ненависть и нетерпимость
- Жестокое обращение с детьми
- Сервисы мгновенных сообщений
- Школьные мошенничества
- Сайты сомнительного содержания
- Неизвестная тематика
- Чаты
- Насилие
- Наркотики
- Азартные игры
- Хакерство
- Нудизм
- Оружие

## Контроль доступа сотрудников

Веб-сайты, связанные с нецелевым использованием интернета на рабочем месте.

- Образование
- Обмен картинками
- Download-архивы
- Персональные сайты
- Отдых и оздоровление
- Здоровье и медицина
- Развлечения
- Мода и красота
- Правительство
- Недвижимость
- Транспорт
- Переводчики
- Поиск работы
- Путешествия
- Рестораны и еда
- Компьютеры и технологии
- Форумы и новостные ленты
- Поздравительные открытки
- Некоммерческие, неправительственные организации
- Потокое мультимедиа и загрузки
- Поисковые системы и порталы
- Частные IP-адреса
- Игры
- Спорт
- Бизнес
- Религия
- Покупки
- Новости
- Политика
- Веб-почта
- Искусство
- Финансы
- Общие

## Другие категории

- Реклама и всплывающие окна
- Детские сайты
- Фондовый рынок
- Форумы с технической или бизнес информацией
- Техническая информация
- Персональные хранилища
- CDN: сети предоставления контента
- Нецензурная лексика
- Профессиональные социальные сети
- Информационная безопасность
- Сайты сомнительного содержания