Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған «Сейфуллин оқулары – 17: «Қазіргі аграрлық ғылым: цифрлық трансформация» атты халықаралық ғылыми – тәжірибелік конференцияға материалдар = Материалы международной научно – теоретической конференции «Сейфуллинские чтения – 17: «Современная аграрная наука: цифровая трансформация», посвященной 30 – летию Независимости Республики Казахстан.- 2021.- Т.1, Ч.4 - С. 127-130

РОДИТЕЛЬСКИЙ КОНТРОЛЬ В СЕТИ ИНТЕРНЕТ

Мәді Е.Т.

Каждая новая технология приносит и волнение, и тревогу. Хотя компьютер и Интернет становятся все более незаменимыми инструментами для детей и имеют много преимуществ в нескольких областях, главным образом в образовании, коммуникации и творчестве, использование компьютера и Интернета также вызывает беспокойство из-за насилия в играх, экстремального использования компьютера, легкости доступа к порнографии и другому противоречивому контенту, вторжения в частную жизнь и интернет-зависимости. Поскольку в настоящее время дети становятся умнее и технологичнее по сравнению со своими собственными родителями, сочетание традиционного метода обучения с технологией помогло вооружить детей навыками, связанными с этой технологией. Несмотря на то, что все эти ранние знакомства с технологией являются хорошей идеей, тем не менее, нам все еще необходимо учитывать способность детей на ранней стадии обучения различать правильное и неправильное. Без надлежащего руководства и наблюдения эти дети могут оказаться в ловушке между удовлетворением, которое может дать технология. Чтобы предотвратить более серьезные случаи, необходимо принять соответствующие меры.

Система мониторинга трафика фактически является одним из реализованных механизмов и может рассматриваться как бэкэнд-процесс для мобильного родительского контроля (РМоС). По сути, эта система интегрирована внутри РМоС с помощью сетевой технологии, такой как программирование сокетов в качестве среднего интерфейса между смартфоном на платформе Android и компьютером, к которому имеет доступ ребенок. Она позволяет выполнять действия для входящего и исходящего трафика с компьютера, используемого ребенком, где она фокусируется в основном на захвате определенного трафика, которым является http-трафик. Весь трафик, к которому ребенок получает доступ, сначала появляется у родителя, и ему необходимо подтверждение, прежде чем он сможет получить доступ в Интернет. Затем, после доступа, весь трафик проверяется и применяется с помощью параметра соответствующие модули системы мониторинга дорожного движения.

Были различные случаи, касающиеся подростков, особенно такие, как побег из дома и слежка за незнакомыми людьми, использование мобильного телефона для отправки коротких сообщений (SMS), скачивание запрещённых видео и изображений, доступ к сайтам без рейтинга и так далее [1]. Все эти действия начинаются с того, что ребенок получает доступ ко всем из них через Интернет, и они считаются нездоровыми и должны быть предотвращены.

В настоящее время мало методик, которые используются для мониторинга трафика. Cisco представляет базовую архитектуру. которая имеет три основных элемента качества обслуживания. Во-первых, идентификация и маркировка QoS методы координации ОКП из конца в конец между сетевыми элементами. Вторым элементом является QoS в пределах одной сети элемент средства постановки в очередь, планирования и формирования трафика. Третий это политика QoS, управление и функции бухгалтерского учета, чтобы контролировать и управлять сквозным трафиком в сети Интернет.

Разработчики представляют разработку и внедрение портативной веб-системы мониторинга и анализа сетевого трафика WebTrafMon. Эта веб-технология позволяет пользователям быть свободными от сложных пользовательских интерфейсов, а результаты мониторинга и анализа можно просматривать из любого места, просто используя широко доступные веб-браузеры. WebTrafMon предоставляет возможности мониторинга и анализа не только для загрузки трафика, но и для типов трафика, источников и направлений. WebTrafMon состоит из двух частей: зонда и просмотрщика. Зонд извлекает из сети необработанную информацию о трафике, а просмотрщик предоставляет пользователю анализируемую информацию о трафике через веб-браузеры. Между тем, авторы описывают, что мобильный агент предоставляет решение для проблемы с программным обеспечением в сетевой среде, которая больше подходит естественно, с реальным миром. Технология мобильного агента может сделать распределённые системы, более адаптируемые к потребностям приложений особенно в мобильной среде.

Разработчики приложения фокусируются на безопасности и разработке приложения на платформе Android с открытым исходным кодом. Также на обеспечении безопасного канала связи с использованием протокола HTTPS. В нем используется инфраструктура открытых ключей, также известная как асимметричное шифрование, например, открытые ключи и цифровые сертификаты. При разработке приложения можно принять концепцию Мобильных приложений (SMA), основанных на сервисе, чтобы преодолеть ограничение, при котором некоторая функциональность выгружается или предоставляется в качестве услуги. Это связано с ограничением ресурса для мобильных устройств, где сложно запускать сложные приложения на устройстве [2]. Кроме того, приложения выполняют коммерческий уровень. Разработка SMA-системы, называемой «Мобильный мат». (MMS), который раскрывает ряд ключевых характеристик, которые являются достойный изучения. Система архитектуры приложения разделена на два уровня: сервер и клиент, использующий архитектуру программирования сокетов для

прослушивания общение, в то время как другой заключается в предоставлении информация. Предлагаемая архитектура действительно решает слабость старой системы видеонаблюдения там, где она была раньше. негибкий.

Родительский мобильный контроль, использующий программирование сокетов в качестве средний интерфейс между Android-смартфоном и компьютером, к которому имеет доступ ребенок. Он позволяет осуществлять деятельность для входящего и исходящего трафика с компьютера, который использует ребёнок, где он фокусируется в основном на захвате конкретного трафика, например, HTTP-трафик. Весь трафик, к которому был получен доступ, сначала будет выглядеть следующим образом: родитель нуждается в подтверждении запроса, прежде чем он сможет получить доступ к Интернету. После доступа, весь трафик проверяется и применяется с соответствующими модулями. Создание прототипа - это процесс разработки временного клона для информационной системы. Таким образом, простой и работающий прототип для пользователя, представляет собой интерфейс и разрабатывается на этапе проектирования, чтобы показать, как ранняя система будет выглядеть для использования приложения.

Преимущество использования прототипной техники состоит в том, что она позволяет разработчикам наблюдать за ранней функциональностью и собирать быстрый отклик. Кроме того, он обеспечивает контроль рисков для разработчиков и пользователей, позволяя проводить раннее тестирование. Прототипирование предлагает множество преимуществ для пользователей и систем. разработчиков, что может помочь избежать недоразумений. Однако быстрые темпы развития могут создать качество проблемы, когда в очень сложной системе прототип мог бы становится трудно управляемым.

Контентная фильтрация домашнего интернета родителями

Для ограничения доступа детей к нежелательному, опасному контенту в настоящее время имеется возможность выбрать как коммерческое, так и свободно распространяемое программное обеспечение, сервисы, тарифные опции Интернет провайдеров, специальные возможности антивирусных программ. Принцип работы этих систем обычно строится на черных (запрещенных) и белых (разрешенных) списках, либо на основе фильтрации. Наиболее широкое распространение получили три алгоритма фильтрации:

1. фильтрация, по ключевым словам, (конкретные слова и словосочетания используются для включения блокировки веб-сайта);

2. динамическая фильтрация (содержимое запрашиваемого веб-ресурса анализируется в момент обращения, загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное);

3. URL-фильтрация (запрашиваемая страница или целый домен, например, dosug.nu, могут быть определены или категорированы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется).

Лучшие в мире системы контентной фильтрации используют URL фильтрацию, основанную на анализе и категоризации Интернет-ресурсов.

Такой механизм признан наиболее эффективным методом фильтрации контента.

Возможности родительского контроля

1. Фильтры web-сайтов. Слова-запреты (фильтры). Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается. Создание белого списка. Более жесткий способ контроля, когда вы самостоятельно составляете белый список сайтов, которые может посещать ребенок. Создание черного списка. В черном списке указываются сайты, на которые ребенку заходить запрещено. Приложение работает с базой данных, где содержатся сайты для взрослых.

2. Ограничение времени, проводимого ребенком за компьютером. Определяйте расписание пользования компьютером и Интернетом: выбирайте допустимое время суток и продолжительность работы. Так вам не придется прогонять ребенка от компьютера и вступать в конфликт - сеанс закончится сам собой.

3. Установка запретов на использование детьми отдельных программ. Во избежание различных недоразумений родители могут ограничить список используемых ребенком программных продуктов. Большинство современных операционных систем имеют в своем составе инструмент доступа пользователей к программным продуктам, что дает возможность ограничения доступа ребенка к нежелательным программным продуктам.

4. Управление доступом к игровым приложениям [3]. Возможности родительского контроля позволяют помочь детям играть в безопасные, дружелюбные, занимательные и обучающие игры, соответствующие их возрасту. В частности, родители могут блокировать как все игры, так и только некоторые из них. Дополнительно родители могут устанавливать разрешение или запрет на доступ к отдельным играм, исходя из допустимой возрастной оценки и выбора типа содержимого.

5. Журнал отчетов о работе ребенка за компьютером. С целью анализа того, чем занимался ребенок за компьютером в отсутствие взрослых, какие программы запускал, какие сайты просматривал в Интернете, с кем общался и т.д., родительский контроль ведет аудит всех действий подрастающего пользователя. В журнал записываются адреса посещенных детьми страниц Интернета. В некоторых программах журнал с отчетом можно получать по электронной почте, что очень удобно, если родитель находится вне дома, и хочет просмотреть, какие сайты посещал ребенок.

Роль семьи не может ограничиваться предоставлением компьютера и интернета своим детям. Семьи также несут ответственность и обязанности по принятию мер предосторожности в отношении своих детей. Они должны установить правила для своих детей относительно определенного поведения онлайн, такого как разговоры о сексе и отправка личной информации тому, с кем они познакомились онлайн, а также должны информировать их о потенциальных опасностях, связанных с такой деятельностью. И они также должны использовать программы ограничения по мере необходимости.

Семьи беспокоятся о том, как обращаться с компьютерами и пользоваться Интернетом, но они не принимают достаточных мер предосторожности. Дети более уверены, чем их родители, в использовании компьютера и интернета, что сказывается на родительских навыках управления этим новым средством. Среди детей 92% утверждают, что чувствуют себя очень или довольно комфортно при пользовании компьютером, по сравнению с 69% их родителей (Livingstone, 2007). Между родителями и детьми существует разрыв в уровне знаний о компьютере и интернете, в частности, между поколениями, при этом дети в большей степени владеют компьютером. Поэтому родителям не очень легко защитить своих детей от вредного содержимого. Соответственно, вероятно, именно в таких ситуациях либо родители не пользуются программами ограничения доступа, либо их программы ограничения доступа могут быть легко дезактивированы детьми. В результате, семьи должны получить знания об использовании компьютера и интернета, а также о возможных способах лечения. Одной из причин неиспользования программного обеспечения ограничения может быть проблема блокирования доступа к образовательным сайтам ошибочно и не позволяет детям осуществлять поиск в интернете в образовательных целях.

Существуют явные доказательства того, что программы фильтрации в некоторой степени предотвращают возможность контакта с порнографией (Mitchell, Finkelhor, & Wolak, 2005). Поэтому может быть полезно, чтобы технические меры предосторожности принимались профессиональными учреждениями, провайдерами Интернет-услуг (Internet Service Providers) или правительством, а не семьями.

СПИСОК ЛИТЕРАТУРЫ

1. Википедия//Родительский контроль - [Электронный ресурс]: https://ru.wikipedia.org/wiki/ Родительский контроль - URL (дата последнего обращения: 18.05.2016 г.).

2. Википедия/Squid - [Электронный ресурс]: https://ru.wikipedia.org/wiki/Squid - URL (дата последнего обращения: 18.05.2016 г.).

3. Гарипова, Г.К. Обеспечение защиты детей от информации, причиняющей вред их здоровью, нравственному и духовному развитию // Августовский семинар учителей-информатиков. - 2013. - № 1. -Б. - 20 с.