Говорим «безопасный Интернет» - подразумеваем eSafe

В целях формирования безопасной Интернет-среды и содействия более ответственному использованию ресурсов глобальной сети, 2009 год был объявлен **Годом Безопасного Интернета**. Данная инициатива, принадлежащая ряду общественных и образовательных организаций, получила поддержку на уровне Министерства связи и массовых коммуникаций РФ. И это вполне логично: построение в России информационного общества невозможно без создания этичной безопасной Интернет-среды, в первую очередь, для такой массовой и в то же время восприимчивой аудитории, как дети и подростки. Согласно данным исследования, проведенного Фондом «Общественное мнение» 4,2 млн. детей и подростков 12-17 лет используют Интернет раз в неделю, а 2,9 млн. – ежедневно. При этом более 60% родителей дают полную свободу в посещении детьми Web-ресурсов, не ограничивая их во времени. На вопрос о том, установлены ли на домашних компьютерах программы фильтрации лишь десятая часть школьников 8-11 классов отвечает утвердительно (См. Рис 1).

Существует несколько способов оградить своего ребенка от просмотра сайтов с нежелательным содержанием (порно, экстремизм, насилие и др.). Самым распространенным из них является родительский контроль (63%), 25% родителей выбирают специальные программы и настройки в браузере и лишь 12% создают специальную «детскую» учётную запись, чтоб ребенок не смог получить доступ к родительским файлам и кэшу браузера, оставшегося в памяти компьютера после работы старших пользователей.

Эксперты в области безопасности выделяют три основные группы наиболее опасных Интернет-угроз (см. Табл. 1), где на 1-ом месте – нежелательный и, более того, противозаконный контент.

Рис 1. Источник: Информационный бюллетень Года Безопасного Интернета. Выпуск 1.

Однако для того, чтобы защитить детей от просмотра непредназначенных для них сайтов, недостаточно просто ограничивать их свободу в использовании ресурсов сети. Сегодня подросток нередко оказывается более грамотным в вопросах настройки ПК и установки соответствующих программ, чем его родители. А значит обход родительских методов защиты это лишь вопрос времени. Как можно оградить детей от опасного контента, с которым им приходится сталкиваться? Существуют ли доступные решения и технологии, позволяющие быть уверенным в том, что общаясь с друзьями или делая домашнюю работу, ребенок не столкнется с неэтичными сайтами и не «насобирает» на свой ПК «букет» вредоносных приложений? Решить большинство этих задач призваны системы контентной фильтрации операторского класса. Их сильная сторона состоит в том, что на конечном устройстве – домашнем компьютере пользователя – не устанавливается никакого программного обеспечения. Все операции по очистке доставляемого тысячам пользователей Web-трафика производятся в сети провайдера Интернет-услуг на уровне шлюза. Таким образом, снижаются риски некорректной установки и настройки клиентского ПО и нивелируются угрозы, связанные с несвоевременным обновлением антивируса. Но самое главное – мамы и папы могут подключать

1.КОНТЕНТНЫЕ РИСКИ	▪ нежелательный контент ▪ противозаконный контент
2.ЭЛЕКТРОННАЯ БЕЗОПАСНОСТЬ	▪ вредоносные программы ▪ спам ▪ кибермошенничество
3.КОММУНИКАЦИОННАЯ БЕЗОПАСНОСТЬ	▪ незаконный контакт ▪ киберспреследования

Табл. 1. Источник: Информационный бюллетень Года Безопасного Интернета. Выпуск 1.

для своих детей услугу «Родительский контроль». В отличие от организационных мер, применяемых родителями, технологическое решение вопроса безопасного использования Web-ресурсов, «обойти» невозможно: ребенок не имеет доступа к управлению средством защиты своего компьютера. Об особенностях технологий контентной фильтрации для провайдеров Интернет-услуг рассказывает **Владимир Бычек**, **руководитель направления Руководитель направления контент-безопасности (eSafe) компании Aladdin**.

– Владимир, в западных странах услуга Интернет-провайдера по доставки «чистого Интернета» на дом достаточно распространена, как обстоят дела с этим сервисом в Росси?

В.Б. Российский антивирусный рынок, как и западный, так же пришел к необходимости предоставления услуг по защите от вредоносного кода и спама на уровне Интернет-провайдеров. Однако, в отличие от западной практики, где наибольшей популярностью пользуется бесклиентская модель предоставления «Родительского контроля» и «Чистого Интернета», в России пока предпринимаются попытки внедрения её аналога клиентского типа, подразумевающего установку стандартного комплекта решений, на стороне пользователя. Такой комплект, как правило, включает персональный антивирус, межсетевой экран, в ряде случаев персональный URL-фильтр («родительский контроль»). Понятно, что среднестатистический абонент не является экспертом по информационной безопасности. Он может неверно понять вопросы персональных средств защиты о разрешении или блокировании неизвестного трафика от его компьютера к какому-либо Интернет-ресурсу. Он не имеет преставления о том, что происходит с программой, которая была изменена либо после обновления, либо в результате инфицирования вредоносным кодом. Эффективность персональных средств защиты против современных угроз также далека от 100%. Ряд угроз не детектируется, значительная часть коммуникаций вредоносных программ также остается незамеченной. Кроме того, персональные средства нагружают компьютер абонента и в ряде случаев делают общение с ним крайне некомфортным для абонента. В итоге, проще отключить антивирусный сканер, чем работать на «тормозящем» компьютере. Такой метод обеспечения услуги безопасного Интернета мы считаем нецелесообразным: пользователь не должен отвечать за то, в чем не разбирается.

- Какие могут быть альтернативы?

В.Б. На наш взгляд, наиболее эффективен подход, при котором обеспечение безопасной работы в Интернет реализуется согласно концепции SaaS (Secure as a Service). В рамках SaaS-модели соответствующие средства защиты размещаются и работают на оборудовании сервис-провайдеров, что позволяет конечным пользователям экономить на покупке и обслуживании ПО и оборудования. Провайдер берёт на себя решение всех вопросов, связанных с безопасной работой абонента в глобальной сети. При этом от самого абонента не требуется ничего, кроме подключения к данному сервису. Таким образом, абонент доверяет решение проблем, в которых не разбирается, оператору, работающему с профессиональным и надежным средством защиты. Безопасность обеспечивается абсолютно прозрачно для абонента, что позволяет ему, не задумываясь над вопросом безопасности, посещать интересующие его ресурсы и не беспокоится за своего ребенка, когда тот «сидит» в Интернете. Вредоносный код отфильтровывается на шлюзе у оператора. Коммуникации «шпионских» программ также блокируются на упомянутом шлюзе. В большинстве случаев абонент даже не подозревает о той работе, которая выполняется для него сервис-провайдером. Одним из примеров такого решения является система фильтрации контента Aladdin eSafe SecureSurfing.

- Расскажите подробнее о возможностях eSafe SecureSurf для абонентов и операторов.

В.Б. Функционал eSafe SecureSurf позволяет оператору предоставлять полный спектр услуг защиты от Web-угроз. К ним могут относиться – «Чистый Интернет» или URL-фильтрация («Родительский контроль») и другие услуги, предоставляемые как физическим лицам, так и компаниям, считающим нецелесообразным приобретение решений для персонального использования. С точки зрения выгоды оператора – это получение дополнительной прибыли и удовлетворение потребности абонентов в безопасном использовании ресурсов глобальной сети. Как следствие повышение лояльности, удержание старых и рекрутинг новых абонентов. Еще один существенный плюс для оператора – снижение нагрузки на службу технической поддержки, а также простота внедрения и гибкое масштабирование системы. Для

абонентов всё еще проще: подключая выбранную опцию, они получают абсолютно прозрачный сервис безопасности, который не требует установки, регулярных обновлений и поддержки. Таким образом, взаимодействие со средством защиты от Web-угроз для пользователя сведено к минимуму. Освободившееся время можно потратить и на более полезные вещи, чем администрирование системы безопасности своего ПК. Например, на воспитательную работу с ребенком. Понятно, что 100% гарантии того, что ребенок не увидит неположенного контента, быть не может. Если задаться целью – любой фильтр можно обмануть. Настоящая задача «Родительского контроля» - оградить детей от случайного попадания на неприемлемые ресурсы. В случае же намеренного поиска «взрослых» сайтов – это будет обнаружено и зафиксировано. Неотъемлемой частью сервиса «Родительский контроль» является возможность получения регулярных отчетов об использовании Интернет. Эти отчеты позволят родителям контролировать сетевые маршруты ребенка и, при необходимости, принимать соответствующие воспитательные меры.

Возможности eSafe SecureSurf

Что может предложить ISP, использующий SecureSurf?

УСЛУГИ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ	УСЛУГИ ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ
ЧИСТЫЙ ИНТЕРНЕТ Данная услуга предполагает: ▪ полную очистку трафика Интернет, передаваемого по протоколам HTTP и FTP от всех видов современного вредоносного кода в реальном времени прозрачно для пользователей. ▪ обнаружение и блокирование коммуникаций вредоносного ПО. ▪ автоматическое перенаправление абонента на заданную web-страницу для очистки ПК от обнаруженного вредоносного кода. РОДИТЕЛЬСКИЙ КОНТРОЛЬ Данная услуга предполагает: ▪ блокирование доступа к web-сайтам Интернет, содержащих информацию, неприемлемую для детей и подростков (порнография, насилие, наркотики, секты и т. д.). ▪ подготовка отчетов для абонентов и выдача их по расписанию либо по запросу.	ЧИСТЫЙ ИНТЕРНЕТ Данная услуга предполагает: ▪ полную очистку трафика Интернет, передаваемого по протоколам HTTP, HTTPS, FTP от всех видов современного вредоносного кода в реальном времени прозрачно для пользователей. ▪ URL-фильтрацию - управление доступом сотрудников Заказчика к web-сайтам Интернет на основе принадлежности сайта к той или иной категории (группе категорий). ▪ блокирование неавторизованных коммуникаций, в том числе зашифрованных, между компьютерами сети Заказчика и Интернет. Детектирование коммуникаций выполняется в реальном времени по сигнатурам протоколов. ▪ управление доступом сотрудников Заказчика к Интернет-приложениям (IM, P2P, потоковое видео/аудио и т. д.). Детектирование приложений выполняется в реальном времени по сигнатурам протоколов; ▪ блокирование нежелательной корреспонденции (спама) с близким к нулю количеством ложных срабатываний и обеспечением очистки легитимного почтового трафика от всех видов вредоносного кода. (обрабатываемые протоколы – SMTP, POP3). ▪ подготовка подробных аналитических отчетов об использовании сотрудниками ресурсов Интернет в нужном разрезе и за определенный период времени. ▪ возможность применения различных политик для рядовых сотрудников и V.I.P.