Точка зрения правоохранительных органов на киберугрозы

написано Александр Астахов | 10 июня, 2023

С точки зрения правоохранительных органов наибольшая угроза со стороны Интернет заключается в предоставляемых ею возможностях глобальных коммуникаций, отслеживать которые чрезвычайно сложно. С целью осуществления перехвата переговоров террористов, осуществляемых с использованием сети Интернет, спецслужбы в настоящее время продолжают расширять штат своих высококвалифицированных ИТ специалистов.

Так, по словам Дона Кавендера, специального агента и инструктора Центра Компьютерного Обучения ФБР, их беспокоит не столько угроза кибертерроризма, сколько использование террористами Интернет для планирования и подготовки физических террористических актов.

Не оставляют равнодушными правоохранительные органы также материалы экстремистского и порнографического характера, используемые, в том числе, и в качестве предлога для установления жесткого контроля над сетью Интернет. Этот контроль у нас в стране воплощается в виде внедрения у Интернет-провайдеров элементов системы проведения оперативно-розыскных мероприятий СОРМ-2, а также в предложениях по разграничению доступа между российским сегментом Интернет (Рунетом) и остальным миром посредством создания системы защищенных шлюзов для фильтрации сетевого трафика.

Поставить шлюз между Рунетом и остальной Сетью (Интернет) предлагает отечественная ассоциация разработчиков ПО. Шлюз, через который будет открываться доступ к зарубежным ресурсам, обойдется в несколько сотен миллионов долларов, а его возведение займет около 10 лет. Авторы идеи полагают, что если

шлюз будет создан, то совсем не обязательно, что он будет использован для ущемления свобод в интернете. Должны быть выработаны международные правила и стандарты отнесения источников информации к опасным для общества и организовано управление национальной сетью на основе диалога государства и сообщества пользователей. При построении отечественного шлюза будет полезен опыт государств, которые уже реализовали такие проекты либо собираются сделать это в ближайшее время, например, Китая, Японии и Сингапура.

Один из самых знаменитых технических ограничителей доступа к глобальным информационным ресурсам реализован в Китае. По сообщению газеты The Epoch Times, «Золотой щит», известный также как «Великий китайский фаерволл» (Great Firewall of China), обошелся стране в $800 млн. (6,4 миллиардов юаней). Близкое к Министерству общественной безопасности Китая издание China News Service полагает, что «Великий китайский фаерволл» включает в себя 640 тыс. серверов.

Китайское правительство последовательно воплощает в жизнь систему тотального контроля интернет-трафика, как входящего, так и исходящего из страны. Эта система, охватывающая всех китайских интернет-провайдеров, получила название «Великий китайский межсетевой экран» или, на мандаринском наречии, «Золотой щит». Многие сайты блокируются этой системой.

«Золотой щит» может обеспечить китайцам значительное преимущество в случае кибервойны в отношении стран с развитой демократией, не допускающей подобного рода цензуры. При необходимости, китайцы могут «перекрыть клапан», полностью изолировав китайский сегмент Интернет от остального мира. По мнению специалистов, для осуществления сетевых атак вероятные противники Китая могли бы в этом случае использовать ботнеты, созданные на компьютерах внутри страны.

На сайте http://www.greatfirewallofchina.org/ можно проверить,

числится ли конкретный сайт в списке запрещенных. Например, наш информационный портал www.iso27000.ru почему-то оказался заблокированным. Видимо, китайский «Золотой щит» работает по принципу минимизации привилегий, по умолчанию блокируя все, что явным образом не разрешено.