К ВОПРОСУ О ТЕХНИЧЕСКИХ РЕШЕНИЯХ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В ИНТЕРНЕТ ПРОСТРАНСТВЕ

Стефачев Алексей Витальевич

магистрант, МПГУ, РФ, г. Москва

TO THE QUESTION OF TECHNICAL DECISIONS OF CO-OPERATION AGAINST AN EXTREMISM IN THE INTERNET SPACE

Aleksey Stefachev

Graduate student of MPGU, Russia, Moscow,

Аннотация. Даная статья посвящена вопросу о системе защитных мер, которые обусловили развитие технологий и программно-аппаратных решений, позволяющие работникам спецслужб противостоять существующей угрозе на пространстве интернет сообществ и обеспечивать эффективные и оперативные действия в целях сохранения безопасности граждан.

Abstract. The article is devoted to the question of the protective measures' system, that leads to development of technologies, software and hardware solutions, that allow security services to confrontation with the existing threat in the Internet communities' space and provide effective and prompt actions in order to preserve the security of citizens.

Ключевые слова: технические решения; противодействие; экстремизм; пространство; интернет; технологии.

Keywords: technical solutions; counteraction; extremism; space; Internet; technologies.

С развитием интернет коммуникаций и широким распространением доступных и высокопроизводительных каналов связи появились новые и существенные риски распространения различных запрещенных материалов и экстремистских сообществ. В обозначенных реалиях, на государственном уровне, была разработана система защитных мер, что в свою очередь обусловило развитие технологий и программно-аппаратных решений, которые позволяют работникам спецслужб противостоять существующей угрозе на пространстве интернет сообществ и обеспечить эффективные и оперативные действия в целях сохранения безопасности граждан.

Ключевым для решения вопроса борьбы с экстремизмом в данном контексте является СОРМ. Система обеспечения розыскных мероприятий (СОРМ), представлена в виде комплекса технических средств и мер, которые предназначены для проведения оперативно-розыскных мероприятий в телекоммуникационных сетях [6]. Изначально, данная система, была обращена к телефонной, подвижной и беспроводной связи и радиосвязи [2].

В 2003 году, Минсвязи России приняло первые документы, которые регламентировали организацию СОРМ на узлах телематических служб и передачи данных. С этого момента система оперативно-розыскных мероприятий получила неофициальное название СОРМ-2. Согласно первому документу «Технические требования к узлам телематических служб и передачи данных для обеспечения проведения оперативно-розыскных мероприятий», были определены область применения и общие функциональные требования. Второй документ «Технические требования к устройству системы технических средств по обеспечению функций оперативно-розыскных мероприятий на узлах телематических служб и передачи данных» посвящен требованиям к средствам для поддержки функций, которые устанавливаются на узлах операторов связи и обеспечивает обработку информации, передаваемой и принимаемой определенными пользователями услуг передачи данных и телематических служб и предоставляет эту информацию к пункту управления. В приложении этого документа подробно описан протокол взаимодействия аппаратно-программных средств СОРМ и передачи данных с пунктом управления, который называется протоколом СОРМ Интернет-ПСИ [2]. Таким образом, к настоящему времени существует государственный инструмент, который позволяет значительно повысить эффективность как внутренних, так и внешних мер по обеспечению безопасности [1]. Можно сказать, что СОРМ-2 использует универсальный механизм перехвата интернет трафика, таким образом обозначаются основные моменты: принимается решение о перехвате IP-сообщений на основе определенных данных, например, кому принадлежит трафик, который должен быть перехвачен; проверяется список зарегистрированных пользователей в базе данных интернет-провайдера, идентифицируются пользовательские данные потенциального нарушителя; находящийся на контроле пользователь проходит процедуру аутентификации и начинает сеанс связи посредством канала интернет-провайдера, а устройство СОРМ в это время производит перехват всех IP-пакетов передаваемых и получаемых пользователем и передает их средствам мониторинга правоохранительных органов [2].

В соответствии с приказом Минкомсвязи РФ №83 от 16 апреля 2014 года с 31 марта 2015 года в силу вступают «Правила применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий». Вышеуказанные правила расширяют перечень контролируемых параметров передачи данных. Теперь кроме IP-адреса под контроль попадают электронные адреса почтовых веб-сервисов, которые не используют средства защиты информации, включая криптографические, идентификаторы служб обмена мгновенными сообщениями, включая ICQ. Кроме этого, данный перечень правил обозначает требование к операторам связи, которое обязывает создать кольцевой буфер, обеспечивающий хранение данных на протяжении как минимум 12 часов. Данное решение неформально называется СОРМ-3 [3].

Поскольку интернет провайдеры являются одним из основных элементов сети передачи данных и осуществляют взаимодействия со спецслужбами в области СОРМ и обязаны обеспечивать доступ в сети интернет в соответствии с законодательством Российской Федерации, то многие крупные компании обеспечили установку оборудования DPI в устройстве собственных каналах связи. Система DPI (Deep Packet Inspection) осуществляет глубокий анализ всех проходящих через нее пакетов. Анализ пакета проходит на верхних уровнях модели OSI. Кроме изучения пакетов по стандартным образцам, которые позволяют однозначно определить принадлежность пакета к определенному приложению, например по форматам заголовков, номерам портов, система DPI осуществляет поведенческий анализ трафика, что в свою очередь позволяет распознавать приложения не использующие уже известные заголовки и структуры данных для обмена данными [8]. Данный метод анализа имеет наиболее высокую точность работы и позволяет однозначно отнести сетевой поток к определенному приложении [4]. Технология DPI позволяет осуществлять точечную блокировку запрещенных материалов [5]. Таким образом, DPI осуществляет не только более глубокий анализ пакетов, но и позволяет наиболее эффективным образом блокировать запрещенный на территории Российской Федерации контент. В свою очередь данные системы мер помогают интернет провайдерам оптимально взаимодействовать с государством в решении вопроса противодействия экстремистским сообществам и прочим нелегальным

элементам в условиях высокоразвитых технологий и ресурсов каналов связи.

Список литературы:

1. Елагин В. С. Законный перехват трафика. А как у них? // Вестник связи. М. 2016.

2. Интерфейсы СОРМ. Справочник / Б.С. Гольдштейн, Ю.С. Крюков, А.В. Пинчук, И. П. Хегай, В. Э. Шляпоберский. - СПб.: БХВ Петербург, 2014. - 160 с.

3. Калигин А. СОРМ в кубе. //Стандарт. 2014 №10.

4. Костин Д.В., Шелухин О.И. Сравнительный анализ алгоритмов машинного обучения для проведения классификации сетевого зашифрованного трафика // T-Comm: Телекоммуникации и транспорт. - 2016. - Том 10. - №9. - С. 43-52.

5. Левшин Н.С. Российские законы как инструмент недобросовестной конкуренции в сфере электронной коммерции // Пробелы в российском законодательстве. - № 5. - 2014. - С. 110-114.

6. Приказ Министерства информационных технологий и связи РФ от 16 января 2008 г. N 6 "Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть I. Общие требования"

7. Пинчук, И.П. Хегай, В.Э. Шляпоберский.— СПб.: БХВ Петербург, 2014. — 160 с.

8. Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Научно-методический электронный журнал «Концепт». – 2015. – № 2 (февраль). – С. 71–75. – URL: http://e-koncept.ru/2015/15039.htm (Дата обращения: 06.10.2017).