Безопасная маршрутизация в Российском сегменте Интернет

Е.С. Сагатов[1], К.Н. Ловцов[1], А.М. Сухов[1]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086

Аннотация. В настоящей работе проанализирована проблема утечки внутрироссийского трафика. Сделана попытка оценить долю внутрироссийского трафика, которая обслуживается на заграничных маршрутизаторах и легко может быть перехвачена. Для анализа качества сетевых соединений предложена и испытана российская система мониторинга NetTestBox. Для выявления аномальной маршрутизации предложен метод пороговых значений для коэффициента эффективности географической маршрутизации. Для каждого направления можно определить порог для величины односторонней задержки, выше которого маршрут необходимо проверять.

1. Введение

Проблема безопасности в российском сегменте Интернет стоит достаточно остро. В отличие от китайского варианта Интернет – Российский сегмент открыт для всех угроз. В том числе и со стороны иностранных организаций и сообществ. Ситуацию усугубляет то, что основные центры управления Интернет: маршрутизация, раздача адресов, правила работы с доменными именами и т.д., управляются организациями, которые находятся за пределами Российской Федерации. На эти организации нет возможности влиять в рамках Российской юрисдикции.

С одной стороны, безопасность российского сегмента Интернет достигается большим числом внешних каналов и сложной структурой. То есть DDoS атаки на переполнение каналов не могут вывести из строя все российские внешние каналы и оказывают разрушающее влияние лишь на последнем, клиентском сегменте сети. Связность с внешним миром при этом не снижается.

Но с другой стороны открытость Российского сегмента Интернет и многочисленные каналы, которые ведут заграницу, делают наш сегмент необычайно уязвимым для сбора трафика. Данная статья посвящена угрозам, связанным с политикой маршрутизации.

Сейчас значительная доля внутрироссийского трафик перенаправляется через зарубежные маршрутизаторы [1], где легко может быть записана и проанализирована. В данной статье делается попытка оценки доли внутрироссийского трафика, которая обслуживается заграницей. Также предлагаются критерии для поиска таких маршрутов и даются рекомендации как можно исправить положение.

Мониторинг и последующее обеспечение безопасности в глобальной сети осуществляются на основе метрик производительности IP сетей (IPPM метрик) [2]. К ним относятся задержка пакетов [3][4], джиттер [5], потери пакетов [6][7] и доступная пропускная способность канала. В настоящий момент существуют несколько инструментов, способных измерять данные

метрики; наиболее распространёнными из которых являются RIPE Atlas [8] и PingER [9]. Мониторинговые узлы этих проектов устанавливаются у Интернет провайдеров по всему миру и постоянно проводят измерения состояния сетевых каналов между собой. Но это всё зарубежные проекты, которые управляются иностранцами.

Финансирование RIPE Atlas осуществляется RIPE NCC самостоятельно за счёт средств, собираемых с провайдеров для поддержания LIR и AS. Так как треть европейских LIR находится в России, то наши провайдеры субсидируют развитие зарубежных измерительных систем. В России в настоящий момент нет своей измерительной системы, позволяющей получать информацию о фактической настройке маршрутов трафика в стране. Это крайне небезопасно, так как позволяет легко уводить любые потоки данных в сети Интернет через иностранные маршрутизаторы.

Нашей командой было разработано российское решение для мониторинга под название NetTestBox, патент РФ №172333 от 18.07.2017 [10]. В отличии от иностранных аналогов данное устройство позволяет измерять одностороннюю задержку пакетов, при этом сохраняя свою миниатюрность, простоту установки, мобильность и низкую себестоимость. На основании значения односторонней задержки пакетов можно легко судить о выходе трафика за пределы российского сегмента Интернет.

В настояще время смонтирована и работает в экспериментальном режиме сеть из четырёх устройств NetTestBox, размещенных в Тольятти, Самаре, Ростове-на-Дону, Москве. Настоящая статья демонстрирует возможности применения инструмента NetTestBox для выявления аномальной внутрироссийской маршрутизации.

2. Измерительные инструменты

Проект RIPE Atlas основан в 2010 году и развивается силами RIPE NCC. Réseaux IP Européens + Network Coordination Centre — один из пяти региональных Интернет регистраторов, отвечающий за европейский сегмент глобальной сети. Для установки миниатюрный датчик RIPE Atlas достаточно подключить к сети с автоматической выдачей (DHCP)настроек и источнику питания по порту USB. Его упрощённая аппаратная часть не позволяет производить измерения крайне важной метрики производительности, односторонней задержки пакетов. Чтобы получить доступ к измерениям, необходимо установить точку RIPE Atlas в своей локальной сети. За функционирование каждой точки ежедневно начисляются баллы, которые можно потратить на проведение измерений. Так же получить доступ к измерениям можно став спонсором проекта. Позволяется снимать показания ping, traceroute, а также проверять состояние систем DNS, SSL сертификаты, HTTP, NTP. На ноябрь 2017 года функционирует 10327 точек (количество колеблется в пределах нескольких сотен точек) в 183 странах.

Проект PingER (Ping End-to-end Reporting) основан в 1995 году сообществом физики высоких энергий. В настоящее время является частью проекта Internet End-to-end Performance Measurement (IEPM), возглавляемого Stanford Linear Accelerator Center (SLAC) и включающая разработки Centre for Applied Network Research, Fermilab, International Centre for Theoretical Physics, Universiti Teknologi Malaysia, Universiti Utara Malaysia и др. Функционал данного измерительного комплекса основан на программе измерения сетевой задержки ping. На основе её измерений вычисляются двухсторонняя задержка пакетов (Round Trip Time, RTT), вариация сетевой задержки (Jitter), потери пакетов. Сайт проекта снабжён огромным количеством сравнительных графиков, диаграмм и таблиц с измерениями, которые находятся в открытом доступе. Дополнительные механизмы позволяют получить информацию о доступной пропускной способности каналов и traceroute между некоторыми точками. На ноябрь 2017 года функционируют 1277 точек на 1097 сайтах в более чем 160 странах.

Проект NetTestBox стартовал 28 июля 2015 года, разработан и управляется командой сотрудников Самарского университета. Проект базируется на микрокомпьютере Raspberry Pi, к которому подключен мультидиаппазонный ГЛОНАСС+GPS приёмник. Для установки миниатюрной точки достаточно подключить её к сети питания и витой парой к сети Интернет. Для работы приёмника необходимо разместить прибор на окне или в любом другом месте уверенного приёма спутникового сигнала. В качестве программного обеспечения используется

операционная система GNU Debian/Linux. ГЛОНАСС+GPS приёмник позволяет с высокой точностью синхронизировать время на всех устройствах NetTestBox, что позволяет проводить измерения односторонней задержки (One way delay, OWD), а не двусторонней, как это делают конкуренты. Так как маршруты туда-обратно часто различаются, информация об односторонней задержке незаменима для аналитики состояния сетей и маршрутизации. На сайте проекта [11] строятся графики для всех метрик производительности IP сетей. Могут быть легко получены табличные данные для дополнительного анализа за прошлые периоды и трассировки маршрутов. На ноябрь 2017 года функционируют 4 точки NetTestBox в Тольятти, Самаре, Ростове-на-Дону и Москве. Сохранены данные по прекратившей работу точке в США.

Для удобства сравнения в таблицу 1 сведены характеристики вышеуказанных измерительных инструментов.

Таблица 1. Характеристики измерительных инструментов.

	Односторонняя задержка пакетов	Двухсторонняя задержка пакетов	Вариация задержки пакетов	Потери пакетов	Доступная пропускная способность	Трассировка маршрутов
RIPE Atlas	–	+	–	–	–	+
PingER	–	+	+	+	+	±
NetTestBox	+	+	+	+	+	+

3. Критерий эффективности географической маршрутизации

Вначале этого параграфа приведем основные сведения о природе сетевой задержке, а также опишем критерий эффективности географической маршрутизации. С математической точки зрения односторонняя сетевая задержка состоит из постоянной части D_{const} и некоторой переменной части D_{var}:

$$D = D_{const} + D_{\text{var}}. \quad (1)$$

С физической точки зрения эту задержку можно описать следующим образом:

$$D = D_{phys} + D_{tel}, \quad (2)$$

где D_{phys} - это время прохождения данных по физическим каналам связи, определяемое скоростью света и специальной теорией относительности, а D_{tel} это телекоммуникационная часть задержки, которая описывается теорией массового обслуживания. В общем случае сетевую задержку можно представить в виде [12]

$$D = D_{\min} + \frac{W}{B} + D_{\text{var}} \quad (3)$$

где $D_{\min}$ - это минимальное значение односторонней сетевой задержки, W - размер пакета, B - доступная пропускная способность канала. При этом всегда выполняется отношение $D_{phys} \le D_{\min}$, то есть мы всегда можем оценить физическую длину маршрута.

В работе [13] для описания эффективности географической маршрутизации были введены понятия телекоммуникационной длины маршрута l_{tel}, географической длины l_g, а также коэффициент эффективности географической маршрутизации k

$$k = \frac{l_{tel}}{l_g} \quad (4)$$

где $l_{tel} \le c_{opt} D_{\min}$ это телекоммуникационная длина маршрута; ее оценка сделана на основе из специальной теории относительности и минимальной односторонней сетевой задержки пакета иду, а l_g это географическая длина между двумя конечными точками маршрута, которую легко определить по карте. Здесь $c_{opt} = \frac{c}{n} \approx 200$ км/мс - скорость света в оптоволокне, так как в качестве среды передачи данных на подавляющей длине маршрута используется оптоволокно.

Следует отметить, что l_g это географическое расстояние между двумя узлами, которую можно измерить по карте. Для оценки внутригородских расстояний, которые необходимы для оценки эффективности точек обмена траффиком вычислить подобное расстояние тяжело, так как узлы точно не привязаны, да и трассы кабельных каналов не известны. Поэтому примем, что длина маршрута внутри города-миллионника равна примерно 150 км, а для столиц Москвы и Санкт-Петербурга это 250 км.

Традиционно, о маршруте принято судить по данным команды *traceroute*, но анализ подобных данных сложен, необходимо привлечение элементов искусственного интеллекта. Тем не менее, наш подход позволяет упростить такой анализ и свести его к анализу единственного числа, значения минимальной сетевой задержки D_{min}.

При нормальной маршрутизации значение коэффициента k для междугородних каналов не превышает 3, а для внутригородских каналов через точку обмена трафиком это значение не может быть больше 5. Поэтому мы можем рассчитать предельное значение минимальной односторонней задержки для соединений между абонентами внутри европейской части России. Если пакеты переправляются по российской территории, то расстояние между абонентами по карте не может превышать 2 000 км, соответственно минимальная задержка будет ограничена 30 мс. Если маршрут заходит в Европу, то географическое расстояние повышается до 5 000 км, при уводе трафика за атлантический океан это расстояние возрастает до 10 000 км. То есть для любого географического маршрута можно рассчитать предельное значение минимальной задержки, при превышении которого можно говорить об аномальной маршрутизации.

В таблицу 2 сведены данные о предельных значениях односторонней задержки, по которым можно определять выход трафика за пределы Российской Федерации.

Таблица 2. Критерий выхода трафика за пределы Российской Федерации.

Маршрут внутрироссийского трафика	Величина односторонней задержки D_{min}
через Европу	≥ 35-70 мс
через Америку	≥ 75-120 мс
по России	≤ 30 мс

4. Точки обмена трафика и их роль в обеспечении безопасности

Точки обмена Интернет-трафиком (Internet Exchange Point, IX) представляют собой сетевую инфраструктуру для обмена трафиком между автономными системами (так называемого пиринга). Операторы связи и другие организации, имеющие свои автономные системы, могут обмениваться трафиком через IX без организации непосредственны каналов друг к другу, а используя канал до точки обмена трафиком.

По данным [14] в России на ноябрь 2017 года организовано 39 точек обмена трафиком. Администраторы автономных систем, подключенных к точкам обмена трафиком, заключают соглашения между собой об обмене трафиком. Следует отметить, что в настоящее время в рамках точек обмена трафиком нет обязательного принципа «все со всеми». Организация обмена происходит в рамках двухсторонних соглашений. Поэтому две автономные системы, включенные в одну точку обмена трафиком, могут быть не связаны напрямую.

BGP (Border Gateway Protocol, протокол граничного шлюза) – это протокол динамической маршрутизации между автономными системами. В этом протоколе пограничной маршрутизации критерием выбора маршрута является политика маршрутизации, которую устанавливает системный администратор. Он решает с кем управляемая им система будет иметь прямой обмен трафиком (пиринг), а с кем нет. Кроме того, настройки BGP предполагают указание основного и резервного внешнего каналов. Данные о внешнем канале и пути доступа к каждой автономной системе заносятся в глобальную таблицу маршрутизации. То есть, обмен между автономными системами в рамках точки доступа может осуществляться на локальном уровне и пользоваться приоритетом. Если же автономной системы нет в списках ближайших соседей, то тогда маршрутизации происходит в соответствии с глобальной таблицей.

Не смотря на указанные недостатки, роль точек обмена трафиком трудно переценить. При правильной настройке маршрутизации доля трафика, который обслуживается вне таких точек, будет стремиться к нулю. Настоящая работа посвящена анализу работы российских точек обмена трафиком, а также выработке рекомендаций, как избежать ситуаций, когда внутрироссийский трафик обслуживается на зарубежных маршрутизаторах.

5. Анализ результатов измерений и пути повышения безопасности маршрутизации

Для того, чтобы проиллюстрировать поиск аномальных маршрутов воспользуемся сначала данными мониторинговой системы NettestBox. Данные об односторонней задержке позволяют выявить не только аномальные маршруты, но также и направления внутри маршрутов, если эти маршруты ассиметричны.

Экспериментальные результаты сведены в таблицу 3.

Таблица 3. Данные о маршрутизации NetTestBox.

	Тольятти	**Самара**	**Ростов-на-Дону**	**Москва**
Тольятти	k / D_{min}, мс	3,1(20,5)	4,6(4,5)	2,7(11,7)
Самара	3,13(20,45)	k / D_{min}, мс	3,5(4,3)	2,2(10,9)
Ростов-на-Дону	23,12(22,52)	17,42(21,45)	k / D_{min}, мс	2,5(2,6)
Москва	11,34(49,74)	10,34(51,74)	12,42(12,77)	k / D_{min}, мс

Ниже диагонали приведены значения минимальной задержки в миллисекундах. Простой взгляд показывает, что на ряде направлений (Тольятти-Самара, Самара-Москва, Тольятти-Москва) эти значения ассиметричны, то есть маршрутизация осуществляется ассиметрично. Кроме того, величина этих значений говорит о том, что маршрутизация, скорее всего осуществляется через Европу.

Проведенное нами дополнительное уточнение маршрута командой *traceroute* подтверждает нашу гипотезу:

Таблица 4. Маршрут на участке Самара-Москва.

Город	**Traceroute Самара->Москва**
Самара	1 big.ssau.ru (91.222.128.24) 0.273 ms 0.366 ms 0.282 ms
Самара	2 sw15-vlan55.ssau.ru (91.222.130.254) 0.538 ms 0.545 ms 0.654 ms
Самара	3 r1-vlan254.ssau.ru (91.222.130.237) 0.666 ms 1.033 ms 1.330 ms
Нижний Новгород	4 79.126.112.69 (79.126.112.69) 18.810 ms 18.872 ms 18.907 ms
Москва	**5 ae40.frkt-cr4.intl.ip.rostelecom.ru (217.107.67.15) 66.486 ms 62.179 ms**
Лондон	**61.126 ms**
Франкфурт	**6 100ge4-1.core1.fra1.he.net (216.66.89.225) 68.474 ms 65.965 ms 66.053 ms**
Москва	**7 fiord-as-as28917…..switch1.fra2.he.net (216.66.87.178) 64.099 ms 67.200 ms**
Москва	**64.054 ms**
Москва	8 msk-m9-b1-xe4-2-1-vlan2049.fiord.net (93.191.9.156) 70.195 ms 66.350 ms
Москва	63.919 ms
Москва	9 as39134-gw.fiord.net (62.140.239.223) 63.587 ms 66.765 ms 66.702 ms
Москва	10 mapripn-gw.exepto.ru (88.212.194.70) 61.069 ms 64.356 ms 65.612 ms
Москва	11 MSK-M9-MR1.Ripn.net (193.232.226.17) 66.832 ms 63.763 ms 66.936 ms
	12 MSK-M9-Relarn-1.relarn.ru (193.232.226.10) 70.577 ms 64.682 ms 68.490 ms
	13 MSK-KHOUSE-Relarn-2.Relarn.ru (194.226.29.181) 68.060 ms 65.211 ms 65.807 ms
	14 nettestbox.relarn.ru (194.190.138.140) 68.027 ms 65.470 ms 68.081 ms

В таблице 3 выше диагонали рассчитаны значения коэффициента эффективности географической маршрутизации k. Данные таблицы подтверждают ранее высказанную гипотезу о предельных значениях коэффициента k.

Следующим шагом попытается оценить долю российских автономных систем, подключённых к точкам обмена трафиком. Сделать это достаточно сложно, найти данные о количестве российских автономных систем или регистраторов (LIR) достаточно тяжело. Не очень понятно даже, есть ли такая статистика у российских органов власти.

Тем не менее, удалось выяснить [15][16], что в России 1930 LIR из 17394 LIR, зарегистрированных в RIPE. Это составляет около 11% от общеевропейского числа, что явилось сюрпризом. Раньше говорили, что в России зарегистрировано треть европейских LIR.

При помощи специально написанного скрипта удалось выявить в базе RIPE NCC 5119 российских AS (IPv4). С учетом того, что общее количество AS, зарегистрированных RIPE немногим больше 36 тысяч (36376) [17], доля российских AS составляет 14%.

Общее количество всех подключений к российским IX составляет 1683 на конец ноября 2017 года, когда были собраны и остальные данные. Следует отметить, что некоторые AS подключены к разным точкам обмена трафика, поэтому реальное число уникальных автономных систем ниже. При этом максимальный охват подключений российских AS к точкам обмена трафика не превышает 32,9%.

Следующие оценки сделаны при помощи измерительной системы RIPE Atlas. Выберем случайным образом по 25 пробников RIPE Atlas в московском и питерском регионах и оценим, сколько их них подключено к соответствующим точкам обмена трафиком. Для Самары и Новосибирска число пробников невелико и процент охвата можно оценить по всем точкам. Полученные данные сведены в таблицу 5.

Таблица 5. Доля автономных систем с датчиками RIPE Atlas, подключенных к точкам обмена трафиком.

№ пп	Регион	Охват
1	Москва	70%
2	С.Петербург	77,8%
3	Самара	50%
4	Новосибирск	75%

То есть, среди автономных систем с датчиками RIPE Atlas доля подключений к точкам обмена трафика намного выше. В среднем в два раза выше, чем для обычной российской AS.

Измерительная система RIPE Atlas позволяет также оценить значение коэффициента эффективности географической маршрутизации для маршрутов между точками, подключенными к точкам обмена трафиком и вне их. Будет также оценена доля аномальных маршрутов, где значение коэффициента превышает 10. Указанные данные удалось собрать только для Москвы и С. Петербурга, они сведены в таблицу 6.

Таблица 6. Статистика коэффициента эффективности географической маршрутизации и доли аномального трафика для автономных систем по регионам.

№ пп	Регион	Значение k		Доля аномальных каналов	
		Внутри IX	Вне IX	Внутри IX	Вне IX
1	MSK	4.08	3.2	8%	5%
2	SPB	5,68	7.26	19,2 %	25 %

В Москве имеется несколько аномальных маршрутов между автономными системами, подключенными к точке обмена трафиком. Это объясняется тем, что не все автономные системы внутри одной точки настроили пиринг между собой. Избирательность представляет собой один из больших недостатков существующей системы. В целом же и значения коэффициента географической маршрутизации, и доля маршрутов с аномальным трафиком выглядят неплохо. В С. Петербурге ситуация с маршрутизацией хуже, что подтверждается обоими показателями.

Для того, чтобы оценить общероссийскую ситуацию нами были выбраны случайным образом 20 точек RIPE Atlas, разбросанных по России, и были проведены измерения задержки между ними. В результате было получено, что доля аномальных каналов по России порядка 6,3%, а пороговое значение коэффициента географической маршрутизации можно принять равным 3,5.

6. Выводы и рекомендации

В результате проведенных измерений удалось показать, что значительная доля внутрироссийского трафика обслуживается на зарубежных маршрутизаторах. Причем для оценки этой доли нам пришлось использовать зарубежные системы мониторинга. То есть национальными средствами мониторинга обнаружить подобные аномалии невозможно.

Тем не менее, российские разработки в этой области имеются, они запатентованы и развернута экспериментальная сеть, которая показала лучшие возможности, чем европейская система RIPE Atlas. В российской системе NetTestBox измеряется односторонняя задежка, что позволяет выявлять аномальные каналы и находить аномальные направления при маршрутизации.

Для проведения мониторинга предложено использовать новый подход, основанный на пороговых значениях коэффициента географической маршрутизации. Такой подход позволит перейти от анализа маршрута к анализу значения односторонней задержки, что очень сильно упрощает мониторинг.

Для решения проблемы локализации внутрироссийского трафика предложено использовать технологию точек обмена трафиком. Существующие точки обмена трафиком имеют существенные недостатки. Во-первых, низкий процент охвата региональных автономных систем. Во-вторых, в рамках каждой точки обмена трафиком не все автономные системы имеют между собой свободный обмен трафиком. В идеале необходимо построение единой общероссийской системы обмена трафиком, где пиринг будет прописан между всеми российскими AS.

Следовательно, для предотвращения ухода внутрироссийского трафика за пределы географической зоны необходимо на законодательном уровне обязать все автономные системы иметь выход к ближайшему IX и разрешать пиринг со всеми автономными системами на этом IX. Это обеспечит прохождение трафика по кратчайшему маршруту. Следует также разработать программу по объединению всех IX магистральными каналами.

7. Литература

[1] Букатов, А.А. Программный комплекс для построения масштабируемых систем IP-телефонии образовательных организаций / А.А. Букатов, А.Н. Березовский, Н.Д. Зайцев, Л.А. Крукиер, А.В. Цимбаленко // Дистанционное и виртуальное обучение. – 2014. – №. 12. – С. 59-70.

[2] IP Performance Measurement (ippm) – [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/wg/ippm/documents/ (17.11.2017).

[3] Almes, G. A One-Way Delay Metric for IP Performance Metrics (IPPM) [Электронный ресурс] / G. Almes, S. Kalidindi, M. Zekauskas, A. Morton // IETF. – 2016. – №. RFC 7679. – Режим доступа: https://tools.ietf.org/rfc/rfc7679.txt (17.11.2017).

[4] Almes, G. A Round-trip Delay Metric for IPPM [Электронный ресурс] / G. Almes, S. Kalidindi, M. Zekauskas, A. Morton // IETF. – 1999. – №. RFC 2681. – Режим доступа: https://tools.ietf.org/rfc/rfc2681.txt (17.11.2017).

[5] Demichelis, C. IP packet delay variation metric for IP performance metrics (IPPM) [Электронный ресурс] / C. Demichelis, P. Chimento // IETF. – 2002. – №. RFC 3393. – Режим доступа: https://tools.ietf.org/rfc/rfc3393.txt (17.11.2017).

[6] Almes, G. A One-Way Loss Metric for IP Performance Metrics (IPPM) [Электронный ресурс] / G. Almes, S. Kalidindi, M. Zekauskas, A. Morton // IETF. – 2016. – №. RFC 7680. – Режим доступа: https://tools.ietf.org/rfc/rfc7680.txt (17.11.2017).

[7] Morton, A. Round-trip packet loss metrics [Электронный ресурс] // IETF. – 2012. – №. RFC 6673. – Режим доступа: https://tools.ietf.org/rfc/rfc6673.txt (17.11.2017).
[8] RIPE Atlas – RIPE Network Coordination Centre [Электронный ресурс]. – Режим доступа: https://atlas.ripe.net/ (17.11.2017).
[9] PingER (Ping End-to-end Reporting) [Электронный ресурс]. – Режим доступа: http://www-iepm.slac.stanford.edu/pinger/ (17.11.2017).
[10] Сухов, А.М. Программно-аппаратный комплекс для измерения метрик производительности IP-сетей: пат. 172333 Рос. Федерация: МПК G 06 F 17/00 (2006.01) / А.М. Сухов, Н.И. Виноградов, Е.С. Сагатов // Заявитель и патентообладатель Самарский университет. – № 2016130896; заявл. 26.07.16; опубл. 04.07.17, Бюл. № 19.
[11] NetTestBox Metrics [Электронный ресурс]. – Режим доступа: http://nettestbox.ip4tv.ru/ (17.11.2017).
[12] Sukhov, A.M. Generating a function for network delay / A.M. Sukhov, M.A. Astrakhantseva, A.K. Pervitsky, S.S. Boldyrev, A.A. Bukatov // Journal of High Speed Networks. – 2016. – Vol. 22(4). – P. 321-333. DOI: 10.3233/JHS-160552.
[13] Sukhov, A.M. Evaluating the effectiveness of geographic routing based on RIPE Atlas data / A.M. Sukhov, A.V. Onoprienko // Telecommunications Forum Telfor (TELFOR), 22nd. – IEEE, 2014. – P. 107-110.
[14] Internet Exchange Map [Электронный ресурс]. – Режим доступа: https://www.internetexchangemap.com/ (17.11.2017).
[15] Local Internet Registries offering service in Russian Federation [Электронный ресурс]. – Режим доступа: https://www.ripe.net/membership/indices/RU.html (19.11.2017).
[16] Total Number of LIRs – RIPE Labs [Электронный ресурс]. – Режим доступа: https://labs.ripe.net/statistics/number-of-lirs (19.11.2017).
[17] 32-bit Autonomous System Number Report [Электронный ресурс]. – Режим доступа: http://www.potaroo.net/tools/asn32/ (19.11.2017).

Secure Routing in the Russian Internet Segment

E.S. Sagatov[1], K.N. Lovtsov[1], A.M. Sukhov[1]

[1]Samara National Research University, Moskovskoe shosse 34, Samara, 443086, Russia

Abstract. In this paper, we analyze the problem of leakage of domestic traffic. An attempt has been made to estimate the share of intra-Russian traffic that is serviced on foreign routers and can easily be intercepted. To analyze the quality of network connections, the Russian monitoring system NetTestBox was proposed and tested. To determine the anomalous routing, a method of threshold values for the efficiency factor of geographical routing is proposed. For each direction, you can determine the threshold for the magnitude of the one-way delay above which the route needs to be checked.

Keywords: traffic analysis, secure routing, autonomous system, AS, Border Gateway Protocol, Internet exchange point, IX.