Андрей Колесников

КРАСНАЯ КНОПКА ИНТЕРНЕТА

«Сегодня телекоммуникации и интернет являются критическими средствами управления государством, фундаментом бизнеса и средством коммуникации между людьми. Важность интернета сложно переоценить», — этой мантрой интернет-бюрократы и чиновники традиционно начинают каждое свое выступление. В этой статье я постараюсь дать простое определение сложных узлов критической инфраструктуры интернета и описать необходимые технические и организационные меры для снижения угроз интернет-инфраструктуре.

ДЕНЬ, КОГДА ГОСУДАРСТВО ОБРАТИЛО ВНИМАНИЕ НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ ИНТЕРНЕТА

Первое серьезное обсуждение критической инфраструктуры интернета на уровне лиц, ответственных за принятие решений, произошло в начале 2009 г. в кабинете заместителя министра связи А. Солдатова. Немногим ранее возросшим влиянием интернета на безопасность озаботился Совет Безопасности России. Мне, как директору *Координационного центра национального домена сети интернет*, вместе с А. Солдатовым, А. Платоновым[1] и рядом других экспертов[2] было поручено определить перечень критических элементов инфраструктуры интернета. Из солидного первоначального списка мы оставили три: DNS-серверы доменной адресации, обслуживающие миллиарды запросов в день, каналы связи и маршрутизация IP-сетей — ключевые составляющие этой основанной на доверии экосистемы[3]. Тогда же, в 2009 г., в контексте обсуждения интернета впервые прозвучало слово *учения*.

В то время в России не было четкого понимания принципов функционирования критической инфраструктуры интернета. Об этом наглядно свидетельствует то, как в 2000-х гг. описывались угрозы. Например, в *Доктрине информационной безопасности Российской Федерации* от 2000 г.[4] технической инфраструктуре, подходящей под определение *интернет,* отводился один абзац: «угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России». В последующем описании этой угрозы всего один пункт имеет отношение к фактически подтвержденным угрозам критической инфраструктуре интернета: «уничтожение, повреждение, радиоэлек-

тронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи». Остальные перечисленные угрозы, такие как «воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации, компрометация ключей и средств криптографической защиты информации», «внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи», «перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации» или даже «использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры» не нашли фактического подтверждения в известных случаях нарушения работы адресной, маршрутной и канальной инфраструктуры интернета в России или других странах.

Вместе с тем, определения из доктрины описывают другие типы атак, направленных не на адресную инфраструктуру и средства маршрутизации, а на конкретные задачи. Например, атаку типа MITM (man in the middle, *атака посредника*)[5], когда подменяются сертификаты безопасности, которыми обмениваются пользователь и интернет-сервер, что делает возможным перехват информации. Замена оригинального сертификата сайта на операторский — довольно распространенная атака в Китае. Однако она не влечет угрозу прекращения работы сети.

За 15 лет принципиальная схема построения инфраструктуры интернета не менялась. Вероятно, не сильно изменится картина и в 2020 г. Тем не менее, сложность и ветвистость Сети возрастает вместе с ролью интернета в нашей жизни. Вероятно, именно поэтому все официальные выступления начинаются с одной и той же мантры.

ОТКЛЮЧИТЬ ИЗВНЕ ИЛИ ИЗНУТРИ?

В конце июля 2014 г. в рамках исполнения поручения Совбеза в министерстве связи и массовых коммуникаций состоялись первые учения по моделированию инфраструктурных угроз интернета. В средствах массовой информации и социальных сетях произошла нешуточная битва между пользователями, опасающимися, что Россия задумала *самоотключиться* от глобальной сети, и технически подкованными специалистами, доказывающими, что моделирование угроз (внешних или внутренних) является нормальной практикой любого ответственного государства или бизнеса[6,7].

В самом деле, планирование и ответственная эксплуатация критических узлов, подготовка регламентов для координации действий всех сторон, вовлеченных в ликвидацию последствий, необходимы вне зависимости от того, вызваны сбои в работе интернета внешними или внутренними причинами.

Для моделирования угроз, а также разработки методов скорейшего восстановления архитектуры, причины, вызвавшие кризис, не важны. Тот факт, что два элемента критической инфраструктуры — генератор файла зоны первичного DNS[8] для выгрузки на корневые серверы DNS и база данных маршрутизации (*Internet*

Routing registry, *IRR*) — размещены на территории США (*ICANN*) и Голландии (*RIPE*) соответственно, зачастую вызывает обеспокоенность у тех, кто опасается политических рисков, но помимо политических конфликтов остается, пусть и малая, вероятность катастрофического физического повреждения инфраструктуры в результате, к примеру, затопления, землетрясения или падения астероида.

Для построения модели угроз и разработки методов снижения рисков будет полезно рассмотреть подробнее критические элементы интернета и построить модели снижения угрозы.

КОРНЕВЫЕ СЕРВЕРЫ ДОМЕННЫХ ИМЕН (ROOT SERVERS)[9]

Доменная адресация построена в строгой иерархии.

В интернете все узлы имеют свой уникальный IP-адрес. Например, 194.67.1.14. Запомнить такие адреса весьма не просто[10]. Поэтому компьютерам, узлам и ресурсам в сети интернет присвоили имена, которые легко запомнить. Система имен DNS отвечает за соответствие доменного имени IP-адресу ресурса и исполняет некоторые другие функции, связанные с адресацией в интернете.

Домен первого уровня, например национальный домен России .RU, отвечает за доменную адресацию в рамках процедур и правил, определяемых национальной регистратурой АНО *Координационный центр национального домена сети интернет*. Домен .GAME принадлежит компании *Uniregistry*. Домен .ORG находится под управлением компании *Public Internet Registry* и так далее. На сегодняшний день в мире используются более тысячи доменов первого уровня, из них порядка 250 принадлежит национальным государствам. Национальные домены верхнего уровня называются ccTLD — country code Top Level Domain. Домены верхнего уровня для общего использования называются gTLD — generic Top Level Domain.

Домены второго и последующих уровней управляются их владельцами. Например, компания *Яндекс* управляет доменами YANDEX.RU, доменами третьего уровня MAPS. YANDEX.RU и MARKET. YANDEX.RU. Количество вложенных уровней не ограничено.

При обращении к интернет-ресурсу по доменному имени подключенное устройство обращается к службе доменных имен DNS и запрашивает IP-адрес, соответствующий этому имени. DNS — весьма динамичная структура. IP-адреса постоянно меняются, но при этом доменное имя остается неизменным.

Серверы DNS в день обрабатывают миллиарды запросов и представляют из себя высоко нагруженную архитектуру серверов, маршрутизаторов и каналов связи. Чтобы максимально быстро обслужить запрос на получение IP-адреса, функции сервера DNS встроены в смартфоны, персональные компьютеры и другие устройства пользователей.

Упрощенная картина архитектуры DNS выглядит так:

- верхний уровень иерархии называется корневым доменом. У него нет формального названия, иногда его обозначают точкой (.). Корневой домен управляется

в рамках исполнения функции IANA корпорацией ICANN и содержит информацию обо всех доменах верхнего уровня. Информация о доменах верхнего уровня размещена на 13 корневых DNS серверах интернета. Эта информация обновляется через *файл корневой зоны*;

- .RU — домен верхнего уровня России, запись с информацией о российских DNS-серверах размещена на корневых DNS-серверах в файле корневой зоны. Внесение изменений в запись осуществляется в рамках функции IANA по заявкам Координационного центра национального домена сети интернет;
- YANDEX.RU — домен второго уровня, таблица с информацией о DNS-серверах Яндекса размещена на серверах RIPN[11]. Внесение изменений в запись на серверах RIPN осуществляются аккредитованными регистраторами. Это российские юридические лица, аккредитованные Координационным центром для регистрации доменов в зонах .RU и .РФ. Информация обо всех доменах второго уровня .RU размещается в *файле зоны .RU.*

В таблице ниже перечислены все 13 корневых серверов, отвечающих за работу системы доменных имен верхнего уровня. Эти серверы обслуживают запросы типа *по какому адресу расположен сервер, отвечающий за функциональность домена .RU?*

Имя хоста	IP адрес	Управление
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	*VeriSign, Inc.*
b.root-servers.net	192.228.79.201, 2001:500:84::b	*University of Southern California (ISI)*
c.root-servers.net	192.33.4.12, 2001:500:2::c	*Cogent Communications*
d.root-servers.net	199.7.91.13, 2001:500:2d::d	*University of Maryland*
e.root-servers.net	192.203.230.10	*NASA (Ames Research Center)*
f.root-servers.net	192.5.5.241, 2001:500:2f::f	*Internet Systems Consortium, Inc.*
g.root-servers.net	192.112.36.4	*US Department of Defense (NIC)*
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	*US Army (Research Lab)*
i.root-servers.net	192.36.148.17, 2001:7fe::53	*Netnod*
j.root-servers.net	192.58.128.30, 2001:503: c27::2:30	*VeriSign, Inc.*
k.root-servers.net	193.0.14.129, 2001:7fd::1	*RIPE NCC*
l.root-servers.net	199.7.83.42, 2001:500:3::42	*ICANN*
m.root-servers.net	202.12.27.33, 2001: dc3::35	*WIDE Project*

Кроме вышеперечисленных 13 серверов в мире действует более 200 зеркал DNS-серверов, которые обеспечивают скорейший отклик для пользовательских DNS-запросов и обеспечивают устойчивость сети корневых серверов в различных регионах. Серверы-зеркала являются точной копией одного из 13 корневых серверов. В России размещены 7 зеркал, обслуживающих запросы пользователей Рунета: копии J, F, L в Москве, K, I в Санкт Петербурге, L в Екатеринбурге и K в Ново-

сибирске. В ответ на запрос *по какому адресу размещена информация о доменах в зоне .RU?* корневой сервер или один из серверов-зеркал ответят:

Имя хоста	IP адреса
e.dns.ripn.net	193.232.142.17 2001:678:15:0:193:232:142:17
f.dns.ripn.net	193.232.156.17 2001:678:14:0:193:232:156:17
d.dns.ripn.net	194.190.124.17 2001:678:18:0:194:190:124:17
b.dns.ripn.net	194.85.252.62 2001:678:16:0:194:85:252:62
a.dns.ripn.net	193.232.128.6 2001:678:17:0:193:232:128:6

Таким образом, узнав, по какому адресу обслуживается домен .RU, запрос клиента *по какому IP-адресу размещен сервер yandex.ru?* будет решаться на серверах доменных имен RIPN.NET, физически размещенных в АО *Центр взаимодействия компьютерных сетей MSK-IX*[12]. Схема, конечно, весьма упрощенная, потому что подавляющее большинство DNS-запросов клиента не выходит за пределы кэширующего[13] сервера местного провайдера.

УГРОЗА DNS

В файле корневой зоны размещена информация обо всех корневых доменах. Предположим, что в силу каких-либо причин выгрузка файла корневой зоны осуществилась с ошибкой в адресе серверов RIPN.NET или с полным отсутствием записи о серверах, обслуживающих корневой домен .RU. Даже при наличии сверхустойчивой архитектуры DNS нельзя исключать технический сбой при выгрузке уникального файла корневой зоны на все 13 корневых серверов. Выгрузка файла зоны осуществляется автоматически по расписанию или при внесении изменений в запись о доменах верхнего уровня (.RU, .COM, .NET и т. д.) соответствующими регистратурами[14] после многоуровневой проверки операторами в схеме работы функции IANA[15] корпорации ICANN[16].

Контроль корректности записей в файле зоны корневых серверов на постоянной основе осуществляет как минимум один российский оператор — упомянутый выше *MSK-IX*. Принцип контроля очень простой: сверяется содержимое файла корневой зоны старой и новой версии. Если в запись о национальных доменах .RU и .РФ внесены несанкционированные изменения, дежурной смене оператора, работающей в режиме 24x7x365, немедленно отправляется уведомление. Кроме того, контролируется объем изменений записей других корневых доменов. Дело в том, что изменения в файл корневой зоны вносятся не часто, и при превышении установленного параметра автоматически формируется уведомление. Схожий метод проверки достоверности выгружаемого файла зоны также используется для контроля внесенных изменений в записи о доменах второго уровня в национальных доменах России. Например, если объем внесенных изменений в файл зоны .RU, полученный от одного из аккредитованных доменных регистраторов, превышает

пороговый параметр, файл зоны не обновляется, и дежурная смена получает соответствующее уведомление.

Если гипотетически возникает ситуация несанкционированного изменения записи о домене верхнего уровня, информация очень быстро распространяется по всем 13 корневым серверам и по всем их зеркалам. Для снижения риска возникновения такой ситуации действует метод поддержки работоспособности с использованием *двойника* корневого сервера с корректной записью о доменах верхнего уровня России. Далее эффективность метода полностью зависит от координации действий ключевых интернет-операторов России. Если в течение короткого времени запись о доменах не восстановлена на корневых серверах, для восстановления работоспособности нужно направить все DNS-запросы *где информация о доменах в .RU?* всех пользователей на территории России на сервер-двойник. Это можно осуществить путем анализа DNS-трафика на сетях операторов и подмены IP-адреса *истинных корневых серверов* на IP-адрес *двойника*, и сделать это нужно по возможности быстро, чтобы информация на кэш-серверах провайдеров также обновилась.

Уже несколько лет *MSK-IX* эксплуатирует корневой сервер-двойник. Однако в случае возникновения ситуации с несанкционированной записью или ее исчезновением из файла корневой зоны DNS, вероятнее всего, во всем мире возникнут сотни *двойников* DNS-серверов, которые будут обслуживать большинство клиентских запросов пострадавшей зоны.

УГРОЗА НАРУШЕНИЯ МАРШРУТИЗАЦИИ ИЛИ ПОТЕРИ СВЯЗАННОСТИ СЕТИ

Второй угрозой, минимизация которой существенно сложнее, является нарушение маршрутизации российских сетей в глобальном интернете. Необходимо подчеркнуть самый важный аспект, из которого проистекает эта угроза. Дело в том, что маршрутизация в интернете осуществляется силами самих участников интернет-отношений. Говоря проще, в интернет-мире не существует регуляций, аналогичных, например, распределению радиочастот. Выделение блоков IP-адресов для операторов и провайдеров осуществляют региональные регистратуры. Их в мире всего пять:

- *American Registry for Internet Numbers (ARIN)* — для Северной Америки;
- *RIPE Network Coordination Centre (RIPE NCC)* — для Европы, Ближнего Востока и Центральной *Азии;*
- *Asia-Pacific Network Information Centre (APNIC)* — для Азии и Тихоокеанского региона;
- *Latin American and Caribbean Internet Addresses Registry (LACNIC)* — для Латинской Америки и *Карибского региона;*
- *African Network Information Centre (AfriNIC)* — для Африки.

Блоки IP-адресов для России выделяет *RIPE NCC,* некоммерческая организация из Нидерландов. Провайдеры и операторы связи самостоятельно обращаются в *RIPE* для получения адресов IPv4 и IPv6. Регистратура никаким образом не влияет на политики маршрутизации операторов и провайдеров. Повторю: операто-

ры и провайдеры во всем мире сами устанавливают политики маршрутизации, т. е. параметры передачи интернет-трафика между оператором А и оператором Б устанавливают эти два оператора. На глобальном уровне интернет-маршрутизация выглядит как конгломерат политик, установленных участниками интернет-отношений, которые объявляют свои политики маршрутизации во внешний мир. Усложняет эту картину мира динамически меняющийся ландшафт маршрутизации, так как в рамках проводимых работ у операторов и провайдеров в таблицы маршрутизации постоянно вносятся изменения. Они фиксируются базой данных маршрутизации (*Internet Routing Registry* — IRR), которая находится под управлением *RIPE NCC*[17]. Это справочная база данных, которой пользуются все операторы и провайдеры, в том числе для определения своих политик маршрутизации.

Существуют две угрозы, связанные с маршрутизацией. Первая — это так называемый взлом протокола динамической маршрутизации или взлом маршрута (*BGP*[18] *hijack*). Хрестоматийным примером такого взлома стал случай *Пакистан против YouTube*[19]. 22 февраля 2008 г. телекоммуникационный регулятор предписал 70 интернет-провайдерам заблокировать доступ к *YouTube* на территории Пакистана. Метод, которым была осуществлена блокировка, заключался в анонсе маршрута на сеть *YouTube* как ближайшего *сетевого соседа*[20] *Pakistan Telecom* для других провайдеров — *сетевых соседей*. Соответственно для пакистанских провайдеров вся сеть *YouTube* была отправлена *в черную дыру*[21]. При этом *Pakistan Telecom* по ошибке анонсировал этот тупиковый маршрут своему внешнему сетевому соседу *PCCW Ltd* из Гонконга. А тот, в свою очередь, являясь одним из крупнейших инфраструктурных провайдеров в мире, не проверил этот анонс и передал его своим международным пирам[22]. В результате 2/3 пользователей *YouTube* в мире (Азия и государства Тихого океана) были отключены от *YouTube*. Проблему обнаружили быстро, анализ ситуации провела компания *Renesys* (ныне *Dyn*), профессионально и на постоянной основе занимающаяся мониторингом маршрутизации в интернете. Среди сетевых инженеров эта ошибка считается *детской*, но время от времени она происходит — чаще по недосмотру, но не исключены случаи злонамеренного перехвата трафика[23]. Через взлом *BGP hijack* можно направить трафик чужого ресурса через свою сеть и проанализировать состав этого трафика. Это серьезная угроза, но она не приводит к разрушению связанности критической инфраструктуры интернета.

Вторая угроза существенно серьезнее — уничтожение информации о маршрутах в базе данных *IRR*. Информация об исчезновении объекта маршрутизации из базы данных *IRR* распространяется не быстро, но по мере обновления таблиц маршрутизации у провайдеров и операторов удаленная из базы *IRR* сеть перестает быть доступной в других сетях. Это непосредственная угроза инфраструктуре.

Проблемы с *кривыми руками*[24] или злонамеренный перехват маршрута *BGP hijack*, как правило, обнаруживают дежурные инженеры. Для рядового пользователя аномалия может снизить скорость передачи данных или, как в пакистанском случае, сделать ресурс недоступным. Обнаружение неправильного BGP-анонса в режиме реального времени и проверка данных IRR на корректность — весьма непростая задача. Во-первых, нужно иметь список всех автономных систем всех российских участников интернет-отношений. Это тысячи записей операторов связи, провайдеров, хостинговых и инфраструктурных компаний, больших

интернет-площадок (*Яндекс, Mail.ru, Google*), банков и т. д. Во-вторых, большинство участников отношений не особо следит за достоверностью маршрутной информации в базе IRR, в этом у них просто нет необходимости, так как соблюдение правильности маршрутов основано на доверии по цепочке между всеми участниками интернет-отношений. В-третьих, для контроля корректности маршрутов необходимо разместить во всех существенных сетях так называемые *пробники* — небольшой и дешевый программно-аппаратный комплекс, который по расписанию запускает тест маршрутизации в проверяемой сети. Эти *пробники* должны передавать данные на центральный сервер, на котором сравнивается предыдущий маршрут с новым, и делаются выводы о корректности маршрута. Построение системы мониторинга маршрутов — это отдельная сложная задача, которую на сегодняшний день реализовали в *RIPE NCC* и в компании *Dyn* (бывшая *Renesys*). Также мониторингом маршрутов и анонсов сетей занимается отечественная компания *Qrator Labs*.

Для ликвидации *BGP hijack* операторы используют метод изоляции сети, которая анонсирует неправильный маршрут. Одновременно технические специалисты связываются с владельцем сети и сообщают об обнаруженных проблемах. Какого-либо единого механизма взаимодействия всех сетей всех операторов не существует по причине тотальной децентрализации.

Удаление данных о маршрутах сети из базы данных маршрутизации *IRR* — еще более серьезная угроза. На сегодняшний день известны только случаи ошибок, когда владелец сети случайно удалял собственные данные. Случаев злонамеренного использования публичной базы данных маршрутизации *IRR* региональной регистратурой *RIPE NCC* не зарегистрировано.

Для снижения угрозы исчезновения данных из базы маршрутизации *IRR* можно использовать точную копию базы данных маршрутизации *IRR*, которой могли бы пользоваться российские операторы сетей и инфраструктуры — этот метод похож на тот, который используется для снижения риска для корневых DNS-серверов. Эта задача решена частично. По имеющейся у автора информации, системы единого мониторинга маршрутизации российских сетей пока не существует.

УГРОЗА ФИЗИЧЕСКОЙ ИНФРАСТРУКТУРЕ

Главным и максимально эффективным средством отключения интернета является физическое отключение каналов передачи данных, которые используются операторами-провайдерами. Не имеет смысла рассматривать модель, в которой сеть оператора или критического узла интернета соединена с внешним миром только одним каналом связи. Такая архитектура в принципе неприемлема для оператора критической инфраструктуры или ресурса.

Определить, какое место занимает то или иное государство по степени устойчивости интернета к угрозам физического отключения, достаточно просто. Общее правило гласит, что чем больше физически независимых каналов соединяет страну с внешним миром, тем лучше. Большая и разветвленная внутренняя архитектура сети в стране поддерживает устойчивость внутри государства. Единый принцип устойчивости сети таков: чем больше операторов и чем сложнее связи между

ними, тем лучше[25]. Безусловно, сложной архитектурой дорого управлять. Однако в модели, где каждый участник интернет-отношений следит за состоянием своей сети, расходы распределяются сообразно размеру каждой сети. Россия входит в число стран-лидеров по устойчивости инфраструктуры интернета. При этом вызывает опасение, что традиционный охранительный подход к защите чего-либо заключается в укрупнении, слиянии и контроле. Централизация и контроль могут сыграть плохую службу для Рунета. Простая логика диктует ответ на вопрос, что проще сломать: распределенную систему со сложными связями или супероператора, через которого проходит весь трафик?[26]

Лекарством от угрозы физического дисконнекта служит наличие множества точек соединения и разнообразие маршрутов при грамотном планировании сетей и надежной коммуникации между операторами при возникновении кризиса.

DDOS-АТАКА

DDoS-атака **я**вляется самым варварским методом нарушения работы инфраструктуры и ресурсов интернета. DDoS может наносить серьезный ущерб всем без исключения сайтам, финансовым и государственным организациям, хостинговым площадкам и провайдерам облачных сервисов. Также DDoS-атаки предпринимаются на DNS-серверы для отказа в обслуживании пользовательских запросов из-за занятости сетевых и вычислительных ресурсов. Принцип работы DDoS-атак описан достаточно подробно. Можно кратко повторить, что злоумышленник отправляет запрос к открытому для публичного доступа интернет-сервису[27], размещенному на мощной инфраструктурной платформе. В запросе, отправленном компьютером под контролем злоумышленника, например к открытому DNS-серверу или серверу точного времени NTP[28], подставляется IP-адрес получателя, куда сервер должен отправить ответ. Так как запрос о домене или точном времени очень маленький, а размер сообщения-ответа от сервера существенно больше, то имея под рукой несколько тысяч зараженных компьютеров, объединенных в ботнет, несколько открытых серверов могут засыпать ответами хороший кусок инфраструктуры, являющийся целью атаки. Этот метод называется *усиление* (amplification).

Мощную атаку хорошего ботнета на цель в сети немедленно видят многие. Страдает ресурс, на который направлена атака. Страдают магистральные каналы и точки обмена трафиком операторов. Первой реакцией оператора может быть остановка маршрутизации по направлениям, откуда приходит атака. Потом наступает время разбора ситуации и ведется поиск источника атаки. Для этого требуется достаточно плотная координация с *сетевыми соседями*. Сегодня все инфраструктурные операторы федерального уровня имеют механизмы контроля DDoS-трафика. У многих применяется технология очистки трафика. Сейчас на рынке появились достаточно качественные сервисные решения по борьбе с DDoS[29].

Перечисленные три угрозы критической интернет инфраструктуре применительно к России можно свести в таблицу:

Угроза	Степень влияния	Лечение	Координация
Удаление записи о домене .RU на корневых серверах DNS или сетевая изоляция корневых серверов для российских сетей	Очень высокая. Нарушения в адресации сайтов и элементов инфраструктуры в домене .RU	Облачная инфраструктура *двойника* корневого сервера под контролем российской компании	Максимальная. Между всеми участниками интернет-отношений и ответственными ведомствами. Необходимо осуществить подмену адресов корневых серверов DNS на адрес *двойника* в сетях операторов связи федерального значения
Нарушение маршрутизации или потери связанности сети — *BGP hijack*, взлом маршрута	Низкая. Возможен анализ трафика перехватчиком	Повсеместное использование средств мониторинга маршрутов российских сетей и постоянный контроль правильности маршрутов самими операторами	Минимальная. Решается оператором взломанного маршрута
Нарушение маршрутизации или потери связанности — удаление записи о сети в базе данных маршрутизации *IRR*	Высокая. Действует не быстро, но верно. Потеря доступности сетей операторов, включая интернет-ресурсы	Мониторинг записей маршрутов российских операторов. Наличие резервной копии базы данных IRR под управлением российского оператора	Максимальная. Между всеми участниками интернет-отношений и ответственными ведомствами. При выявлении аномалий в маршрутизации — переключение на резервную российскую базу данных IRR
Угроза физической инфраструктуре	Высокая. Мгновенное отключение от интернета целых регионов. При авариях внутри страны — потеря связанности сетей	Чем больше маршрутов и каналов, тем лучше. Заранее продуманные политики маршрутизации между ведущими российскими операторами	Максимальная. Между существенным числом участников интернет отношений и ответственными ведомствами. При возникновении аварий на физической инфраструктуре возникает необходимость переключения на резервные каналы
DDoS-атака	От низкой до высокой	Отражение атаки на пограничных рутерах[30]. Очистка трафика	Средняя. Плотная работа с операторами — сетевыми соседями, от которых *льется* DDoS-трафик

С развитием инструментария для мониторинга элементов критической инфраструктуры интернета каждый оператор по мере сил устанавливает средства контроля собственных критических узлов. Вместе с тем, быть готовым к серьезному кризису означает заблаговременную подготовку сценариев реагирования и регулярные тренировки по их исполнению. Для этого должны быть задействованы многие интернет-игроки, отвечающие за функции критической инфраструктуры. В первую очередь. это касается операторов связи и провайдеров адресной и информационной интернет-инфраструктуры. Главным элементом успешной ликвидации глобальных аварий на интернет-инфраструктуре являются проработанные сценарии и отлаженная координация.

КООРДИНАЦИЯ — ГЛАВНЫЙ ЭЛЕМЕНТ ЗАЩИТЫ ИНФРАСТРУКТУРЫ

Существует два метода координации. Первый, децентрализованный, действует в рамках неформального общения ответственных инженеров операторов связи, провайдеров и операторов интернет-инфраструктуры. При отсутствии катастрофических аварий или злонамеренных отключений эта схема в полной мере реализована в России и других странах.

Второй метод, кризисный, должен быть реализован на государственном уровне, так как разрушительное воздействие на интернет-инфраструктуру государства может быть вызвано весьма серьезными причинами, требующими государственного контроля по определению. Вывод о том, что координация является ключевым элементом схемы противодействия угрозам критической инфраструктуры интернета, достаточно очевиден. Посмотрим, что нам в ближайшее время предложит государство.

Сегодня в России действует несколько центров реагирования на сетевые угрозы. В их число входит *RU-CERT*, старейшая группа экспертов, занимающаяся координацией сетевых угроз в России и за рубежом. Существует государственный *GOV-CERT*, группа в рамках ФСБ, реагирующая на угрозы, связанные с государственными ресурсами в сети интернет. *GIB-CERT* организован компанией *GROUP-IB*, профессионально занимающейся сетевыми инцидентами, взломами и анализом криминальных действий злоумышленников. Также центр реагирования на инциденты работает в Роскомнадзоре. Перечисленные центры работают в рамках неформальных связей с операторами и провайдерами, а также с площадками хостинга и информационными ресурсами. В настоящее время методы взаимодействия интернет-акторов при критических авариях в сети не закреплены правом и нормами. Также ничего не известно о регламентах такого взаимодействия. Хотя в контексте поручения Совета Безопасности подготовка таких регламентов и законодательных актов — это первый и необходимый шаг, который должен быть предпринят со стороны государства.

СКРЫТЫЕ УГРОЗЫ

Стоит вкратце упомянуть другие угрозы сетевой инфраструктуре, о которых часто говорят, но которым нет фактических подтверждений.

Перехват маршрутизации или полное отключение взаимодействия сетей. Теоретически эти действия можно осуществить, имея недокументированные функции

в главных магистральных маршрутизаторах (*задняя дверь*, *back door*). Обладая этой информацией, группа злоумышленников может удаленно выключить интернет в отдельно взятой стране. Ходят не подкрепленные фактами слухи, что таким образом был отключен интернет в Сирии.

Задняя дверь в алгоритме шифрования RSA. Этот стандарт шифрования используется в 99% всех устройств в интернете. Так как стандарт является американским, ходят слухи, что в самом алгоритме существует *закладка*, позволяющая перехватывать и расшифровывать информацию. Этот устойчивый миф, так как закладки бывают не в алгоритме, который легко повторить и проверить. Но они встречаются в *обвязке* к математике — как на аппаратном уровне, так и на уровне программ.

Подводные лодки обрежут оптоволоконные кабели, соединяющие континенты[31]. Эта статья наделала много шума. Но основными реакциями на публикацию были недоумение и смех. Интернетом пользуется весь мир, и разрушение одного такого кабеля не нанесет ущерба отдельно взятой стране.

Несмотря на разнообразие, разветвленность и динамическую маршрутизацию интернет-трафика, угрозы базовой инфраструктуре адресации и маршрутизации, а также риск физического отключения должны быть приняты в расчет при построении моделей противодействия угрозам. Причины, которые могут вызвать глубокий интернет-кризис в отдельно взятой стране, не столь важны для специалистов, в обязанность которых входит ликвидация последствий. Даже полная передача контроля над функциями IANA из-под юрисдикции США в руки прогрессивного мирового интернет-сообщества или под управление правительств не даст 100%-ной гарантии от ошибки в записи в файле корневой зоны DNS. Наличие новых регуляторных требований по наведению порядка с учетом автономных систем российских операторов и крупных интернет-площадок не даст гарантии от удаления блоков сетей из базы данных IRR. База эта основана на добровольной передаче информации о собственных маршрутах участников интернет-отношений. Защита инфраструктуры должна быть основана на глубоком понимании архитектуры и уязвимостей, а также на четких сценариях и отработанных практикой действий главных участников интернет-отношений в России.

Что делать, если перестал работать интернет в городе, в области, в стране? Вероятно, к этому моменту также перестала работать мобильная связь и наблюдаются перебои в работе фиксированной связи. Это непременно приведет к некоторому коммунальному коллапсу, так как системой мобильной передачи данных пользуются различные службы.

Рядовому пользователю придется просто ждать, пока инженеры восстанавливают связь. Инженеры канальной инфраструктуры и специалисты по маршрутизации непременно установят между собой контакт и будут совместно латать бреши в инфраструктуре.

Огорчает, что не существует единого телефонного номера центра реагирования на угрозы интернет-инфраструктуре. Конечно, инженеры сделают все от них зависящее, чтобы восстановить Рунет, воспользовавшись наработанными частными связями. Представляется, что создание единого центра координации и есть главный вывод, который должен получить Совет Безопасности России по результатам

учений 2014 г. Отработки сценариев должны продолжаться с учетом наличия такого центра.

Примечания

1 А. А. Платонов, генеральный директор АО *Технический центр интернет*. Ранее директор РОСНИИРОС, под контролем которого находились серверы домена .RU, — RIPN.NET.

2 Также над вопросом в разное время работали М. Якушев (ICANN), Д. Бурков (RU-CENTER, RIPE). Активное участие в работе группы принимали И. Химченко и О. Чутов из министерства связи.

3 Провайдеры и операторы интернета, не связанные друг с другом контрактными обязательствами, пропускают трафик между пользователями и ресурсами третьих сторон. Это ключевое правило, позволяющее интернету быть глобальным. Фундаментом доверия выступают интернет-протоколы.

4 Доктрина информационной безопасности Российской Федерации, 9 сентября 2000 г. http://www.scrf.gov.ru/documents/5.html

5 Атака посредника, Википедия https://ru.wikipedia.org/wiki/Атака_посредника

6 «Совет безопасности обсудит отключение России от глобального интернета» — Ведомости http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet

7 «Совет безопасности обсудит отключение России от глобального интернета» — Коммерсантъ http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet

8 Серверы имен DNS https://ru.wikipedia.org/wiki/DNS-сервер

9 Корневые серверы интернет http://www.root-servers.org/

10 Сегодня имя домена исполняет две функции: адресную и маркетинговую. *Красивые* домены обладают повышенной стоимостью, как часть бренда компаний.

11 RIPN — это английское название АНО *Российский научно-исследовательский институт развития общественных сетей* — РОСНИИРОС.

12 На самом деле RIPN.NET — это не отдельно стоящий сервер, а *облако*, с использованием протокола anycast обеспечивающее кратчайший отклик с точки ближайшего сетевого присутствия. Аналогично устроены и корневые серверы, и серверы обслуживающие национальные домены (.RU, .RS, .AZ и т. п.), и домены общего пользования (.COM, .ORG, .MUSIC и т. п.). Доступность сервиса RIPN.NET — 100%, т. е. перерывов в обслуживании за более чем 20-летний срок работы не было.

13 Кэширующий сервер DNS — сервер, пропускающий через себя DNS-запросы клиентов. Сервер поддерживает актуальную таблицу соответствия имени домена и IP-адреса во всех доменных зонах, тем самым обеспечивая скорейший отклик на запрос клиента из его сети.

14 Администратором (регистратурой) национальных доменов .RU и .РФ является АНО *Координационный центр национального домена сети интернет*

15 Internet assigned numbers authority https://www.iana.org/about

16 Внесение изменений в записи о корневых доменах является частью функции IANA, которую исполняет выделенное подразделение ICANN.

17 RIPE Internet Routing Registry FAQ https://www.ripe.net/manage-ips-and-asns/db/faq

18 Border Gateway Protocol https://ru.wikipedia.org/wiki/Border_Gateway_Protocol

19 Pakistan causes YouTube outage for two-thirds of world http://abcnews.go.com/Technology/story?id=4344105&page=1 ABC news

20 Сетевой сосед — оператор или провайдер, с которым имеется соединение и осуществляется маршрутизация интернет-трафика.

21 В данном контексте *black hole* — распространенный (и весьма варварский) способ фильтрации по IP-адресам.

22 Peer (пир) — примерно то же самое, что и *сетевой сосед*.

23 Someone's Been Siphoning Data Through a Huge Security Hole in the Internet http://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/ — Wired

24 Кривые руки — мягкий и весьма распространенный термин среди технического сообщества.

25 Syria, Venezuela, Ukraine: Internet Under Fire http://research.dyn.com/2014/02/internetunderfire/

26 Минсвязи не допустит повторного массового отключения интернета в Азербайджане http://www.trend.az/business/it/2459139.html

27 Для DDoS-атак используются открытые сервисы DNS и точного времени.

28 Сервер NTP https://ru.wikipedia.org/wiki/NTP

29 Например, *Qrator Labs* http://qrator.net/ru/. В сети *Ростелеком* установлено средство защиты *Arbor* и применяются средства очистки трафика для клиентов.

30 Пограничный маршрутизатор (border router) установлен на границе сети оператора/провайдера и подключен либо к международному провайдеру, либо к точке обмена трафиком с другими операторами.

31 Russian Ships Near Data Cables Are Too Close for U.S. Comfort http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=1