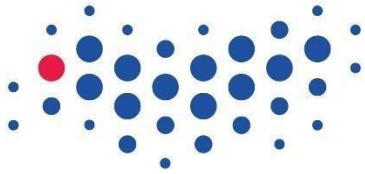
Министерство науки высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет «инфокоммуникационных технологий»

Направление подготовки «11.04.02 Инфокоммуникационные технологии и системы связи»



УНИВЕРСИТЕТ ИТМО

Реферат

«Обзор технологий обеспечения безопасности протокола BGP в сети Интернет»

Выполнили:

Белоцерковец С.А. К41101

Блохнин А.А. К41111

Зиятдинов Р.М. К41101

Филянин И.В. К41111

Проверил:

доцент, к.т.н.
Грудинин В. А.

г. Санкт-Петербург

2021

Оглавление

Список сокращений и условных обозначений 3

Введение 4

1 Краткая характеристика протокола BGP 6

2 Актуальные угрозы стабильности работы сети Интернет на основе протокола BGP 8

3 Обзор современных технологий обеспечения безопасности работы протокола BGP 11

Заключение 16

Список используемых источников 17

Приложение А 19

Приложение Б 20

Приложение В 21

Приложение Г 22

Список сокращений и условных обозначений

ЛВС – локальная вычислительная сеть;

ЦОД – центр обработки данных;

AS (англ. *Autonomous system*) – автономная система;

BFD (англ. *Bidirectional Forwarding Detection*) protocol – протокол обнаружения двунаправленной пересылки;

BGP (англ. *Border Gateway Protocol*) – протокол граничного шлюза;

EGP (англ. *Exterior Gateway Protocol*) – протокол внешнего шлюза;

IANA (англ. *Internet Assigned Numbers Authority*) – Администрация адресного пространства Интернет;

IETF (англ. *Internet Engineering Task Force*) – инженерный совет Интернета;

IGP (англ. *Interior Gateway Protocol*) – протокол внутреннего шлюза;

IP (англ. *Internet Protocol*) – межсетевой протокол;

ISO (англ. *International Organization for Standardization*) – Международная организация по стандартизации;

OSI model (англ. *The Open Systems Interconnection model*) – модель взаимодействия открытых систем;

PI (англ. *Provider Independent*) addresses – провайдеро-независимый блок адресов;

RFC (англ. *Request for Comments*) – рабочее предложение;

RPKI (англ. *Resource Public Key Infrastructure*) — иерархическая система открытых ключей (PKI);

RIR (англ. *Regional Internet Registry*) - региональный интернет-регистр;

RR (англ. *Router Reflector)* - отражатель маршрутов для iBGP спикеров внутри AS.

Введение

Подключение к сети Интернет играет жизненно важную роль в различных сферах деятельности человека: бизнесе, обучении, государственном управлении и т.д. Множество существующих технологий предполагают отправку трафика различного типа между узлами сети Интернет, что привело к его конвергенции – по одному и тому же пути пользователи получают услуги доступа в Интернет, телевещания, голосовой передачи, а также ряд различных персональных сервисов. Помимо этого, с развитием программного и аппаратного обеспечения, объем трафика значительно увеличился, появилась необходимость его фильтрации, приоритиразции, эффективной пересылки.

Существующие протоколы маршрутизации оказались неспособными ответить необходимым требованиям гибкости и функциональности, поэтому был разработан протокол динамической междоменной маршрутизации BGP, на сегодняшний день являющийся одним из основных механизмов, обеспечивающих функционирование сети Интернет. Однако, несмотря на неоспоримые преимущества, протокол BGP не обеспечивает встроенную верификацию маршрутной информации, соответственно, возникают риски искажения, ошибок, сверхутилизации трафика или его кража. Таким образом, вопросы использования наиболее эффективных технологий обеспечения безопасности работы протокола BGP являются важнейшей ветвью развития данного протокола, что и обуславливает *актуальность* данной темы исследования.

Объектом данного исследования является протокол маршрутизации BGP, а *предметом* исследования – методы и средства обеспечения его защиты от атак и угроз работоспособности различного типа.

Целью данного исследования является изучение актуальных угроз безопасности протокола BGP, обзор и обоснование наиболее эффективных методов и технологий их устранения.

Задачи исследовательской работы:

1. Исследование предметной области и ее проблематики. Построение плана научно-исследовательской работы. Формулировка и подготовка полученных данных к использованию и возможному внедрению.

2. Формулировка основных принципов работы протокола BGP в сети Интернет.

3. Описание существующих сетевых угроз безопасности работы протокола BGP.

4. Обзор существующих технологий защиты от атак и угроз безопасности работы протокола BGP.

5. Оценка эффективности приведенных методов обеспечения безопасности.

Используемые методы исследования в данной работе: библиографический анализ литературы в области информационных систем и технологий, международных стандартов и спецификаций и материалов сети Интернет.

Данная работа состоит из 21 страницы, содержит 2 таблицы, 1 рисунок и 4 приложения.

1 Краткая характеристика протокола BGP

Основным назначением протокола BGP является обмен информацией о доступности сетей между всеми участниками BGP-пиринга (от англ. peering – соседство). В качестве основной обменной информации, используемой в данном протоколе, выступают маршруты до определенной адресной подсети (именуемыми также префиксами) и закрепленной за ней автономной системой. Под автономной системой понимается система взаимосвязанных IP-сетей, находящаяся под единым управлением и строго определённую политику маршрутизации в сети Интернет.

Принципы и конфигурация работы протокола BGP значительно отличается от IGP протоколов. Во-первых, маршрутные данные, переданные автономной системе (или, говорят, «анонсируемые») содержат совокупность атрибутов, определяющих оптимальность того или иного маршрута до сети назначения, причем данные атрибуты описывают не технические характеристики пути передачи данных (как например джиттер, задержка или величина пропускной способности), а на значения приоритетов и политик маршрутизации. Помимо этого, протокол BGP является единственным протоколом маршрутизации, способным обрабатывать большие объемы маршрутных данных – на начало 2021 года размер таблицы маршрутизации сети Интернет составлял 855 800 маршрутов (*Приложение А*).

BGP является формализованным протоколом, поскольку распространением номеров AS занимается IANA, делегирующая свои полномочия между пятью RIR в различных регионах всего мира. Ответственным RIR в Европе и Российской Федерации является RIPE NCC, он же и закрепляет PI-блоки адресного пространства IPv4 или IPv6 за определенной автономной системой. В RFC 4893 определен новый, 32-битный диапазон ASN, обеспечивающий существование до 4 294 967 295 номеров AS и правила указания атрибута Aggregator [11].

iBGP - реализация протокола BGP, работающая внутри AS. Основное назначение – резервирование и обеспечение связности для передачи маршрутов внутри сети AS. BGP-пиры устанавливают TCP сессии по 179 порту напрямую без автоматического обнаружения спикеров [6]. Маршрутные данные приходят в сообщениях типа «update» и могут содержать ряд атрибутов пути в зависимости от степени их обязательности (таблица 1) [7][8]:

Таблица 1-1. Описание характеристик BGP выбора пути

Атрибут	**Приоритетность при выборе маршрута**[1]	**Назначение**
Well-known mandatory — распознаются всеми маршрутизаторами и присутствует во всех сообщениях во всех update-сообщениях.		
Next-Hop	0 (проверка доступности)	IP-адрес следующего маршрутизатора для достижения AS назначения
AS path	2 (наименьшее число AS)	Совокупность AS до сети назначения (стек)
Origin	3 (IGP > Incomplete)	Указание на метод получения маршрута: IGP, или указана вручную при конфигурации
Well-known discretionary — распознаются всеми маршрутизаторами, но их присутствие в update-сообщениях не обязательно.		
Local preference	1 (максимальное значение)	Указывает маршрутизатору приоритет выхода внутри AS (значение по умолчанию в сетях Juniper – 100)
Atomic aggregate	-	Указывает на то, что NLRI является агрегированным
Optional transitive — могут не распознаваться всеми маршрутизаторами BGP, и update-сообщение либо принимаются, либо отправляется другому пиру с сохранением данного атрибута.		
Communities	4 (в зависимости от значения ASN:COM)	Определяет политику маршрутизацию трафика и тегирование маршрутов, существуют резервированные значения
Aggregator	-	Совокупность RouterID и local AS
Optional non-transitive — могут не распознаваться всеми маршрутизаторами BGP, и update-сообщение либо принимается, либо отбрасывается.		
MED	5	Информирует пиров о предпочтительности маршрутов
OriginatorID	6	Указывает RouterID (не являющийся RR), который анонсируется маршрут внутри AS
ClusterListID	7	Указывает список кластеров для RR, помогает избежать петли между iBGP-пирами

[1] Актуально для сетей Juniper. При наличии eBGP-спикера Cisco, наиболее приоритетным является параметр *weight*: не передается в update и предпочтительность пути тем выше, чем выше значение данного параметра.

2 Актуальные угрозы стабильности работы сети Интернет на основе протокола BGP

Протокол BGP уязвим к различным сетевым атакам, под влиянием которых маршрутная информация становится недостоверной или искаженной. В результате таких нарушений большое количество пользователей сети Интернет становятся недоступны, а часть маршрутов может быть захвачена нелегитимными узлами BGP сессий, что зачастую приводит к высоким временным и финансовым потерям крупных международных компаний. Основной причиной таких инцидентов является тот факт, что протокол BGP не имеет встроенных механизмов верификации соединений и шифрования передаваемых атрибутов и NLRI (Network Layer Reachability Information).

Наиболее распространённым нарушением в работе протокола BGP является перехват префиксов (именуемый также BGP hijacking).

Основная суть данной угрозы заключается в повреждении таблиц маршрутизации путем отправки ложных сообщений BGP UPDATE, которые содержат атрибуты пути и префиксы, а также значения keepalive/hold timers, регулирующие сеанс BGP. Значения данных атрибутов не соответствует реально существующим, или соответствуют значениям ложного BR (border router, пограничный маршрутизатор). Таким образом, злоумышленник манипулирует потоком трафика, а также путем широковещательной рассылки о префиксах распространяет собственную информацию базу маршрутизации (RIB, Routing Information Base) одноранговым BGP-пирам, в другие AS [2]. Не всегда перехват IP-префиксов является преднамеренным – возможны ошибки в конфигурации магистрального оборудования на сети провайдера, например:

- от имени AS анонсируется чужой префикс/от имени чужой AS анонсируется префикс (*Приложение Б*):

- от имени AS анонсируется more-specific префикс чем тот, который анонсируется «родной» AS;
- от имени AS анонсируется маршрут с более предпочтительным AS-path.

Еще одним типом атак на работоспособность BGP является атака типа «отказ в обслуживании» (DOS). При данной атаке отправляется большое количество ложного трафика, что приводит к высокой нагрузке на сетевое оборудование [5]. В результате данной атаке становится недоступен маршрутизатор-участник BGP сессии, в результате чего все участники обмена маршрутами не получит сообщения keepalive, в результате сессия переходит в состояние ‘Active’, соединение становится нестабильным и необходимые маршруты жертвы может не анонсироваться в другие автономные системы. Также известны ситуации, когда основная линия резервирована, однако hello и keepalive пакеты приходят с задержкой, ввиду этого происходят падения BGP-сессии по причине «чувствительных» BFD таймеров, что, разумеется, является лишь следствием из атаки данного типа [12].

BGP Man-in-the-Middle (BGP MitM) – угроза, основное назначение которой является отслеживание и возможный перехват потока трафика злоумышленниками [4][15]. Данное нарушение происходит, когда маршрут, ранее являющейся резервным, становится основным через маршрутизатор злоумышленника. А ввиду того, что протокол BGP изначально не предоставляет никаких средств шифрования или аутентификации трафика, атрибуты маршрутов становятся открытыми, появляется возможность реализовать так называемый Traffic Interception. Угроза такого типа является сложно осуществимой ввиду необходимости не только понимать алгоритмы функционирования протокола BGP, но и изучить за период короткий времени принципы достижимости и иерархии маршрутизации между целевыми AS.

Помимо этого, распространена ошибка типа «утечка маршрутов» (англ. *route leaks*), когда от имени какой либо AS анонсируется полностью легитимный маршрут, по которому должен перенаправляться трафик высокого класса обслуживания, на данном маршруте обеспечиваются необходимые пропускные ресурсы. Однако из-за некорректной настройки пиринга, данный маршрут может также анонсироваться в совершенно ином направлении , и он в таком случае выступает лучшим по ряду параметров (например, меньшее число AS-хопов), хоть и нежелательным путем направления трафика. Таким образом, возникают возможные проблемы задержки или потерь трафика, проходящего через «незапланированную» сеть провайдера (рисунок 2-1).

Таким образом, протокол BGP, несмотря на его уникальность и гибкость в конфигурации, при неправильной его эксплуатации может повлечь за собой потенциальные проблемы маршрутизации не только внутри локальных автономных систем, но и в целом в глобальной сети Интернет. На сегодняшний день ряд вендоров сетевого оборудования, как например, Juniper Networks или Cisco Systems, предлагают инструменты строгой фильтрации маршрутов и детальной обработки и анализа входящих пакетов на основе применённых внутренних политик.

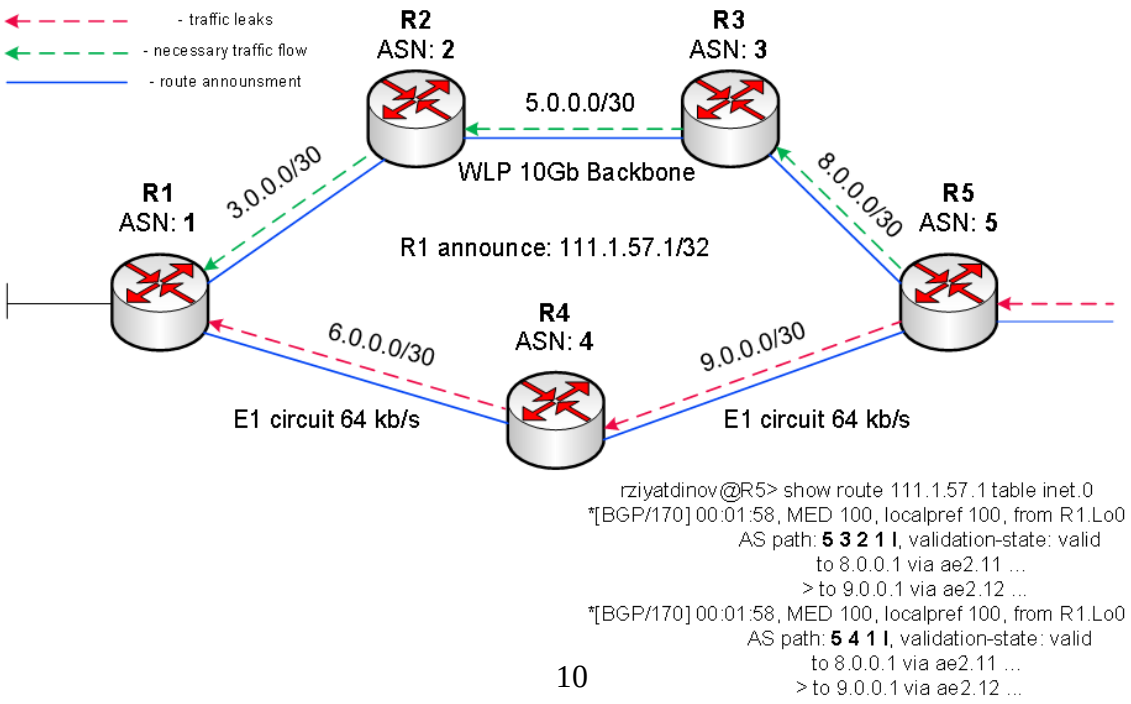


Рисунок 2-1. Иллюстрация ошибки route leaks

3 Обзор современных технологий обеспечения безопасности работы протокола BGP

Наиболее эффективным способом борьбы с перехватом префиксов (BGP hijacking) является использования механизмов фильтрации. Например, Cisco предоставляет алгоритмы фильтрации на (NLRI, Network Layer Reachability Information) основе информации о доступности подсетей, однако наиболее общим в сети Интернет для всех операторов Tier-1 и Tier-2 является использование инструмента RPKI на стыках различных магистральных операторов связи.

RPKI — иерархическая система открытых ключей, разработанная и реализованная с целью обеспечения безопасности глобальной маршрутизации в сети Интернет. RPKI основана на стандарте X.509 и спецификациях RFC3779 и RFC528, описывающие процесс аутентификации BGP-источников маршрутной информации путем предоставления цепочки криптографических сертификатов при распределении Интернет-ресурсов между автономными системами, демонстрирующих владение заданным блоком адресов (или даже единственным /32 префиксом). Ресурсы последовательно выделяются несколько организаций:

IANA (Internet Address Number Authority) – администрация адресного пространства интернета. Интернет-ресурсы изначально принадлежат IANA, она управляет пространствами IP-адресов для доменов верхнего уровня. Она же присваивает номера для автономных систем (AS) – систем IP-сетей и маршрутизаторов, которыми управляют операторы связи. Эти номера AS необходимы для маршрутизации.

RIR (Regional Internet Registry) – региональные интернет-регистраторы, IANA распространяет ресурсы через них. Всего их 5 для разных регионов – RIPE NCC, ARIN, APNIC, AfriNIC, LACNIC.

LIR (Local Internet Registry) – локальные интернет-регистраторы, как правило, крупные сервис-провайдеры. RIR распространяет ресурсы на LIR’ы, которые уже распределяют их между своими клиентами.

Доверенным центром сертификации RPKI для владельцев AS выступает IANA, сами сертификаты располагаются в публичных RPKI репозиториях у всех RIR в так называемых «точках доверия», они в свою очередь – для LIR [1]. Сертификаты хранятся в базе данных, по которой можно проверять достоверность информации. Базы данных расположены на публичных репозиториях RPKI у всех RIR – на так называемых «точках доверия», или Trust Anchors.

Чтобы подтвердить безопасность ресурсов, их владельцы создают с помощью сертификатов криптографически заверенные объекты, или ROA.

ROA (Route Origin Authorisation) – это объект с цифровой подписью, который подтверждает, что конкретная AS имеет право быть источником какого-то маршрута и анонсировать его в интернете. Запись ROA имеет 3 параметра:

- номер AS, которая является источником маршрута;
- префикс и его длина (это IP-адрес с маской: xxx.xxx.xxx.xxx/yy);
- максимальная длина префикса.

Понятно, что проверка анонсируемых префиксов может быть реализована каждым RPKI-маршрутизатором, однако такой подход не рекомендован, так как требует большой траты ресурсов маршрутизатора (ресурсоемкие криптографические операции при получении данных RPKI), а альтернативной для него является добавление собственного RPKI-сервера, который может синхронизировать свою базу с публичными RPKI репозиториями. Таковой кэш-сервер генерирует базу данных, состоящую из записей типа префикс + ASN, и периодически обновляет ее магистральных маршрутизаторах через защищенное TCP соединение (8282) по протоколу RPKI-RTR.

На маршрутизаторе полученная база данных формирует RV (route validation) записи, состоящие из: самого префикса, origin-AS (AS-источник) максимальной длины префикса (листинг 1).

Листинг 1. Пример RV

```
RT.OV.SPB> show validation database
RV database for instance master

Prefix              Origin-AS Session                    State   Mismatch
1.0.0.0/24-24          13335 172.31.7.4                    valid
```

Эта запись используется для проверки каждой записи в таблице FIB, с которым совпадает поле префикс RV записи: префикса, максимальной длинны указанной в RV записи и соответствие номера AS (*Приложение В*). В итоговом случае, полученный от eBGP-пира анонс префикса может быть принять настроенные состояния, принятые RPKI RIPE (таблица 3-1) [9][10].

Таблица 3-1. Состояния полученных префиксов по RPKI RIPE Validator

Состояние	**Обозначение**	**Действия**
valid	На анонсируемые префикс и origin-AS присутствует RV-запись	Принимается, передается
invalid	На анонсируемый префикс найдена RV-запись, однако отмечено несоответствие origin-AS или длины префикса	Не принимается, не передается
unknown	На анонсируемые префикс и origin-AS присутствует RV-запись	Принимается, не передается

Наиболее распространённым инструментом обеспечения DOS-stable является применение на стыках с downlink-пирами определенных правил – community – которые, в соответствие с политикой маршрутизации данной AS применяют ряд фильтрующих параметров к принимаем анонсам. Так, например, префикс анонсируемый с community «ASN:666» у большинства операторов - «черная дыра», то есть позволяющая отвести поток трафика еще на входе в сеть автономной системы [6]. Следует отметить, что такая система «блекхолинга» довольно гибкая и позволяет реализовать исключение UDP-трафика или UDP-усилителей (*Приложение В*).

Помимо RPKI-валидации, которая является необязательным, а только рекомендованным инструментов, многие сервис-провайдеры осуществляют

фильтрацию анонсируемых префиксов с использованием объектов route (или же, *route object*) через *IRR* (Internet Routing Registriest) – это распределенная база данных маршрутизируемой информации, используемая при отладке, настройке и проектировании Интернет-маршрутизации в сети Интернет. IRR предоставляет механизм для проверки содержимого объявлений маршрутов или сопоставления исходного номера AS со списком сетей. Для этого владельцу автономной системы с блоком выделенных адресов необходимо выполнить техническую координации совместно со своим RIR, а именно:

1. Создать необходимые типы объектов в БД своего RIR;

2. Зарегистрировать собственную политику маршрутизации на языке RPSL в БД (это может быть RIPE, RADB, ARIN и т д).

После этого, осуществляется пере конфигурация магистральных маршрутизаторов поставщика в соответствии с значениями объектов в базе данных (Приложение Г).

IRR отображают весьма неполную картину, так как регистрация данных в этих базах данных сугубо добровольная.

Многие операторы не хотят себе морочить голову какими-то IRR, часть операторов не регистрирует по причине нежелания разглашать свою политику. Те же, кто все же зарегистрировал свою политику, не всегда поддерживают актуальность данных.

Магистральные провайдеры для пресечения фабрикации адреса источника трафика, и, как следствия, DOS-атак используют внутренние системы фильтрации (ACL в Cisco-системах или различные RouteMaps), ориентированные либо на ручной настройке фильтров на пограничных маршрутизаторах с неявным отклонением, либо на передаче от BGP-спикера правил фильтрации (IP FlowSpec), что позволяет автоматически управлять трафиком, приходящим от пира в соответствии с типами NLRI и набором правил и действий валидации (rate-liniting, redere и т.д). (*Приложение В*) [14].

Также возможна реализация шаблонно-ориентированных (mitigation) инструментов защиты (как, например, система Arbor), которые

ориентируются на стандартный эскиз потока трафика и отслеживают аномалии при усилении какого-либо его типа. В таком случае, выполняется детальная обработка пакетов на основе 12-ти параметров (ICMP Type, TCP flags, Port и т.д.) описанных в стандарте RFC 5575 [13], что является методом приоритезация типов трафика для клиентов и услуг типа «IP-транзит».

Для решения проблемы перехвата анонсов или трафика должны быть решены две основные задачи:

- аутентификация принадлежности пограничного маршрутизатора определённой AS;

- контроль целостности маршрутных данных.

Для обеспечения вышеприведенных требований устанавливают соединения между двумя BGP-партнёрами с использованием каналов IPSec (с алгоритмом шифрования DES) и алгоритмом хеширования TCPMD5 [3][16].

Однако, несмотря на все преимущества данного подхода, его реализация также находится под сомнением. Проблема при установлении BGP over IPSec связана необходимостью в регулярном обновлении открытых IKE-ключей, деинкапсуляции пакетов, их пересылки, что в свою очередь, может потребовать от маршрутизатора выделения больших вычислительных ресурсов (NVRAM), увеличения нагрузки на ASIC (для различных типов маршрутизаторов) и возрастание очередей к ControlePlane элементам маршрутизатора. Таким образом, время re-key (обмена и обновление ключей) синхронизации между двумя IPSec спикерами может быть значительно выше, чем значение BGP hold timer, что, несомненно, приведет к частым падениям BGP-сессий и несоблюдению SLA.

Заключение

В данной работе были рассмотрены наиболее частые уязвимости в работе протокола BGP, а также представлены основные подходы, помогающие российским и международным провайдерам связи Tier-2 и Tier-1 уровня усовершенствовать сходимость и безопасность протокола BGP для дальнейшей работы в сети Интернет.

Стоит отметить важную особенность данного протокола маршрутизации – его уникальность и гибкость. Данные свойства обеспечиваются наличием большего числа параметров выбора лучшего пути, возможностью однозначно определить отношения и состояний соседства между участниками протокола BGP, а также наличием дополнительных расширений, реализованных в рамках других протоколов: например, Multiprotocol BGP, использующийся в сетях MPLS VPN, или BGP Flowspec, позволяющий оперативно распространить пирам правила применения политик и firewall-фильтров для конкретной автономной системы.

В ходе исследования определено, что слабым местом протокола BGP является установка и верификация сессии обмена маршрутными данными между BGP-пирами. На стыках двух BGP-соседей становится важным авторизовать принадлежность IP префиксов конкретной AS для корректной отправки маршрута. На примере работы данного протокола маршрутизации можно представить себе степень незащищенности глобальной сети Интернет при несанкционированном вмешательстве в работу ее поддерживающих служб.

Список используемых источников

1. Muhammad Mujtaba. Analysis of BGP security vulnerabilities. - University of Technology Sydney, 2012. – p. 204-214.

2. А.С. Гирев. BGP HIJACKING. - Программно-техническое обеспечение автоматизированных систем, 2019. – С. 133-135.

3. А.В. Козачок. Обеспечение безопасности BGP. – Информационная безопасность, 2011. – С. 553-560.

4. RFC 4271. A Border Gateway Protocol 4 (BGP-4). [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 2006. – Режим доступа: https://www.ietf.org/rfc/rfc4271.txt, свободный. – яз. англ.

5. RFC 4272. BGP Security Vulnerabilities Analysis. [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 2006. – Режим доступа: https://tools.ietf.org/html/rfc4272.txt, свободный. – яз. англ.

6. RFC 4274. BGP-4 Protocol Analysis. [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 2006. – Режим доступа: https://tools.ietf.org/html/rfc4274, свободный. – яз. англ.

7. RFC 1997. BGP Communities Attribute. [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 2006. – Режим доступа: https://tools.ietf.org/html/rfc1997, свободный. – яз. англ.

8. Bahaa Al-Musawi, Philip Branch. BGP Anomaly Detection Techniques: A Survey. - IEEE Communications surveys & tutorials, 2016. – p. 3-4.

9. Гадасин Е.В., Веденеев П.С., Шведов А.В. Уязвимости системы маршрутизации глобальной сети интернет и возможные пути их преодоления – Перспективные технологии в средствах передачи данных, 2019. – С.94.

10. BGP User Guide. Juniper TechLibrary [Электронный ресурс] / Juniper Networks. – Электрон. текстовые данные. – 2020. – Режим доступа: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-routing/config-guide-routing-bgp.html, свободный. – яз. англ.

11. RFC 4893. BGP Support for Four-octet AS Number Space. [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 2007. – Режим доступа: https://tools.ietf.org/html/rfc4893, свободный. – яз. англ.

12. Font of all knowledge. [Электронный ресурс] / RETN company. – Электрон. текстовые данные. – 2020. – Режим доступа: https://foak.retn.net/, закрытый. – язык англ., рус.

13. RFC 5575. Dissemination of Flow Specification Rules. [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 2009. – Режим доступа: https://tools.ietf.org/html/rfc5575, свободный. – яз. англ.

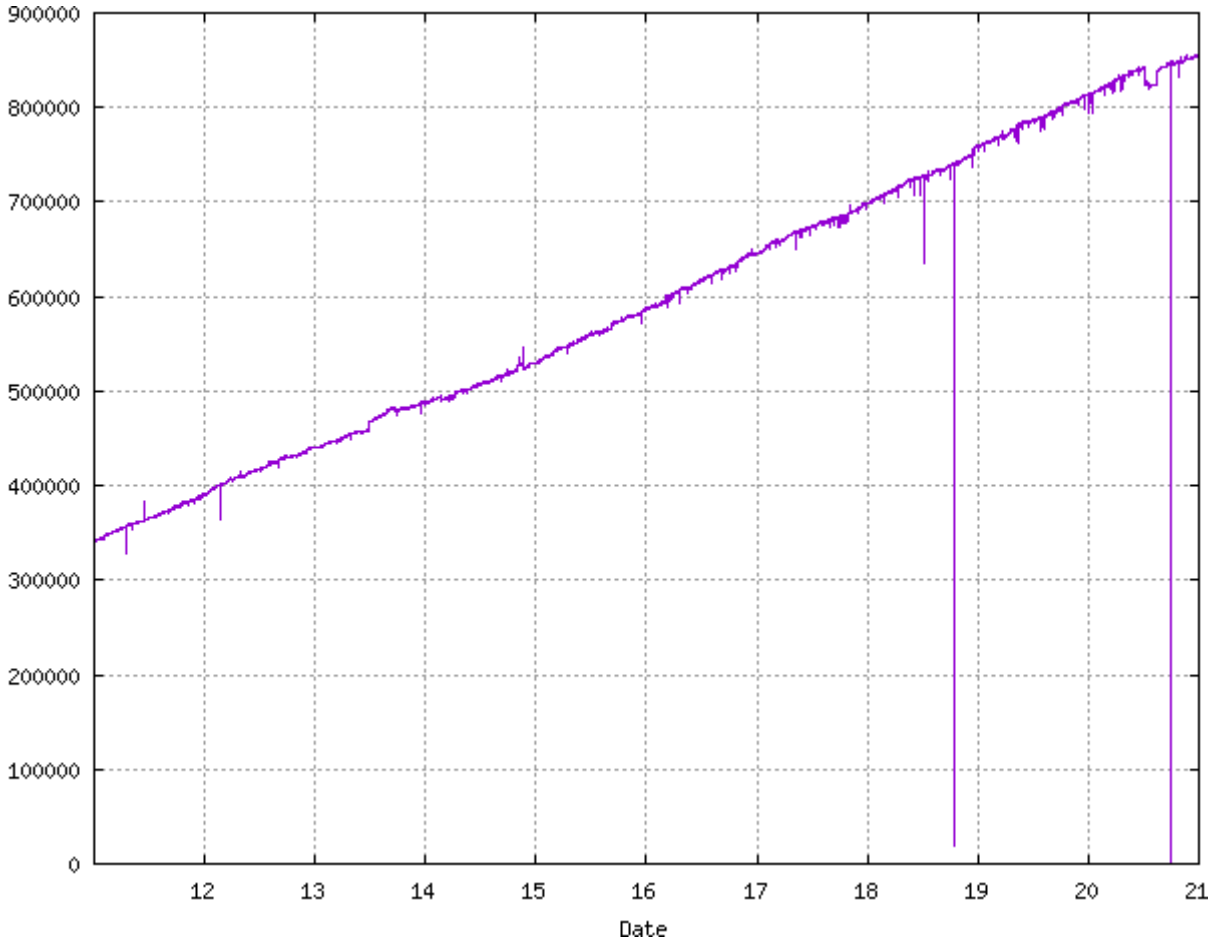
14. RFC 4760. Multiprotocol Extensions for BGP-4. [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 2007. – Режим доступа: https://tools.ietf.org/html/rfc4760, свободный. – яз. англ.

15. Devikar R.N. Impact of MRAI timer on BGP updates and convergence time. / Indonesian journal of electrical engineering and computer science, 2018. – p. 873-882.

16. RFC 2385. Protection of BGP Sessions via the TCP MD5 Signature Option [Электронный ресурс] / IETF. – Электрон. текстовые данные. – 1998. – Режим доступа: https://tools.ietf.org/html/rfc2385, свободный. – яз. англ.

Приложение А

Рисунок А-1. Размер FIB сети Интернет с 01.01.2011 до 01.01.2021



Приложение Б

Листинг Б-1. Пример правильной конфигурации на маршрутизаторе

```
RT.OV.SPB> show route receive-protocol bgp 87.245.250.79 table inet.0

inet.0: 823207 destinations, 1786150 routes (822972 active, 268091 holddown, 268 hidden)
  Prefix              Nexthop              MED     Lclpref    AS path
* 77.234.192.0/19     87.245.250.79        20                 42289 I

RT.OV.SPB> show route 77.234.192.1 table inet.0

inet.0: 823346 destinations, 1786495 routes (823110 active, 268510 holddown, 268 hidden)
+ = Active Route, - = Last Active, * = Both

77.234.192.0/19    *[BGP/170] 7w1d 00:12:21, MED 100, localpref 200
                      AS path: 42289 I, validation-state: unknown
                    > to 87.245.250.79 via ae1.461

$ whois -m 77.234.192.1
route:          77.234.192.0/19
descr:          ITMO University
origin:         AS42289
notify:         noc@itmo.ru
mnt-by:         VUZTC-MNT
created:        2007-01-29T11:47:27Z
last-modified:  2020-01-20T15:00:40Z
source:         RIPE
```

Листинг Б-2. Пример неправильной конфигурации на маршрутизаторе – ложное значение origin AS

```
$ whois -m 193.161.204.0
route:          193.161.204.0/24
origin:         AS51765
mnt-by:         EUHOSTFI-MNT
mnt-by:         CREANOVA-HKI-MNT
created:        2020-12-21T12:34:33Z
last-modified:  2020-12-21T12:34:33Z
source:         RIPE

RT.OV.SPB> show route receive-protocol bgp 87.245.250.79 table inet.0 hidden | match
193.161.204.

inet.0: 823207 destinations, 1786150 routes (822972 active, 268091 holddown, 268 hidden)
  Prefix              Nexthop              MED     Lclpref    AS path
* 193.161.204.0/24  87.245.248.34        100                212871 I

RT.HMO.HKI> show route 193.161.204.1 table inet.0 hidden detail

inet.0: 822961 destinations, 1645066 routes (822961 active, 2369 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

193.161.204.0/24   *[BGP/170] 2w3d 02:35:56, MED 100, localpref 200
                      AS path: 212871 I, validation-state: invalid
                    > to 87.245.248.34 via ae0.201
```

Приложение В

Листинг В-1. Пример настройки политик для проверки префиксов (с соответствующей RV записью)

```
RT.EQX.FKT> show configuration policy-options policy-statement check_rpki term valid
from validation-database valid;
then {
    validation-state valid;
    community add origin-validation-state-valid;
    reject;
}

RT.EQX.FKT> show validation database | match 1.6.184.0/22
1.6.184.0/22-22            9583 172.31.7.4                        valid

RT.EQX.FKT> show route protocol bgp validation-state valid
1.6.184.0/22       *[BGP/170] 1w3d 10:55:29, MED 150, localpref 100, from 87.245.224.161
                      AS path: 1299 9583 I, validation-state: valid
                    >  to 87.245.232.234 via ae3.4
```

Листинг В-2. Пример настройки входящих FlowSpec-фильтров на маршрутизаторе Juniper

```
RT.EQX.FKT> show configuration routing-options flow | display set
edit routing-options flow ddos
set from destination-address A.B.C.D/32 protocol udp source-port 123
set then discard
```

Листинг В-3. Пример анонса префикса с community ASN:666

```
RT.NTL.KIV> show route receive-protocol bgp 87.245.237.50 hidden detail 91.250.9.155

inet.0: 825266 destinations, 1925075 routes (825178 active, 345841 holddown, 520 hidden)
  91.250.9.155/32 (3 entries, 1 announced)
     BMP: Pre: advertise Station: EBHS
     BMP: Pre: advertise Station: EBHL
     Nexthop: 87.245.237.50
     AS path: 6712 I
     Communities: 9002:666
     Hidden reason: rejected by import policy

RT.NTL.KIV> show route 91.250.9.155 table inet.0

inet.0: 825268 destinations, 1925152 routes (825182 active, 345996 holddown, 513 hidden)
+ = Active Route, - = Last Active, * = Both

91.250.9.155/32    *[BGP/170] 00:14:02, MED 100, localpref 20, from 172.31.7.2
                      AS path: 6712 6712 6712 6712 I, validation-state: unverified
                    to Discard
                    [BGP/170] 00:14:02, MED 100, localpref 20, from 172.31.190.2
                      AS path: 6712 6712 6712 6712 I, validation-state: unverified
                    to Discard
```

Приложение Г

Листинг Г-1. Проверка принадлежности префикса к БД RIPE NCC

```
whois -m 45.227.252.0/24 | grep source
source:         LACNIC

 45.227.252.0/24 (2 entries, 0 announced)
    BMP: Pre: advertise Station: EBHS
    BMP: Pre: advertise Station: EBHL
    Nexthop: 87.245.239.175
    AS path: 43201 43201 43201 29031 58271 209272 I
    Communities: 8631:100 12389:20 12389:7130 12389:8020 29031:21011 43201:0
    Hidden reason: rejected by import policy
```