# РЕШЕНИЕ ДЛЯ АВТОМАТИЗИРОВАННОГО ВЫЯВЛЕНИЯ И ПРЕДУПРЕЖДЕНИЯ АНОМАЛИЙ МАРШРУТНОЙ ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ ПО ПРОТОКОЛУ BGP-4

## AUTOMATIC DETECTION AND DISTRIBUTION PREVENTION OF INCORRECT BGP-4 ROUTING INFORMATION

***A. Mansurov***
***D. Schetinin***

*Summary.* Route leaks and route hijacking are the most known actions that cause severe problems for BGP-4 routing and affect the overall connectivity and reliable operation of the Internet. The proposed solution enables automatic identification of route leaks and hijacked routes relying on the information from the Internet routing registries. The solution does not require modification of current software of BGP-4 routers of a monitored telecom carrier. Routes being identified as suspicious or malicious are effectively blocked by the proposed solution thus preventing further distribution of such routes by the monitored telecom carrier and affecting its directly connected neighbors.

*Keywords:* Border Gateway Protocol (BGP-4), BGP seecurity, network security, routing, telecom carrier.

***Мансуров Александр Валерьевич***
*К.т.н., доцент, ФГБОУ ВО «Алтайский государственный университет», Россия, г. Барнаул*
*mansurov.alex@gmail.com*
***Щетинин Даниил Сергеевич***
*ФГБОУ ВО «Алтайский государственный университет», Россия, г. Барнаул*
*1nta4r@gmail.com*

*Аннотация.* Сбои и аномалии в распространяемой по протоколу BGP-4 маршрутной информации дестабилизируют связность операторов и непосредственно влияют на функционирование всей сети Интернет. Предлагаемое в работе автоматизированное решение по выявлению и предупреждению аномальной маршрутной информации позволит предотвратить нарушение легитимных путей обмена данными и не допустить эскалации проблемы на уровне сетевого взаимодействия других операторов, связанных с контролируемым предлагаемым решением оператором связи. Решение использует информацию из баз данных регистратур маршрутной информации сети Интернет и не требует модификации программного обеспечения для поддержки новых безопасных реализаций протокола BGP-4.

*Ключевые слова:* Border Gateway Protocol (BGP-4), сетевая безопасность, безопасность BGP, маршрутизация, оператор связи.

## Введение

С позиции технического межсетевого взаимодействия множество автономных систем (АС), составляющих современную всемирную сеть Интернет, образуют связность друг с другом при помощи пограничных для каждой АС маршрутизаторов и используют протокол маршрутизации BGP-4 (Border Gateway Protocol ver. 4) для обмена маршрутной информацией друг с другом [1] (при этом в качестве АС понимается набор маршрутизаторов, находящихся под единым административным управлением, использующих протокол внутрибоменной маршрутизации, а также единый согласованный план маршрутизации и согласованную картину адресатов, доступных через данную АС). Протокол BGP-4 используется с 90-х годов XX века и, благодаря своей надежности и операционной гибкости, является основой межоператорского взаимодействия по сегодняшний день.

К сожалению, с момента своего появления, протокол BGP-4 был ориентирован на решение непосредственных вопросов обеспечения оптимальной маршрутизации между АС, и практически минимально обращал внимание на проблемы безопасности своей работы, что, с течением времени, привело к достаточному количеству глобальных сбоев и нарушению нормальной работы всего межоператорского взаимодействия [2,3]. Согласно статистике, собираемой веб-ресурсом BGPmon, ежедневно регистрируется около 35 инцидентов, негативно влияющих на общую связность телекоммуникационных сетей, использующих протокол BGP-4 как основной метод взаимодействия друг с другом и обмена маршрутной информацией [4]. Среди наиболее характерных проблем можно выделить банальные ошибки конфигурирования маршрутизаторов АС, участвующих во взаимодействии друг с другом по протоколу BGP-4 (что часто встречается у операторов связи разного масштаба по различным причинам), а также «утечки» и «угоны» маршрутов (когда

маршрутные префиксы той же самой длины или более мелкие/специфичные анонсируются от имени другой АС — случайно или преднамеренно).

За последние 15–20 лет было выполнено большое количество исследований с целью повысить надежность работы протокола BGP-4 и исключить появление обозначенных ранее проблем [2–3,5–9]. Авторами исследований были обозначены несколько направлений, суть которых заключалась в корректировании работы стандартного алгоритма принятия решений протокола BGP-4 при получении маршрутной информации. Ключевыми среди всех предлагаемых решений можно обозначить следующие моменты:

1. Выявление аномалий в маршрутной информации путем анализа самого маршрута-префикса и его атрибута AS-PATH.
2. Включение специальных криптографических подписей-хешей, позволяющих установить подлинность самого распространяемого маршрута-префикса и легитимность его пути распространения.

Анализ маршрута-префикса и его атрибутов может выполняться независимо от работы самого алгоритма протокола BGP-4, результаты анализа могут быть использованы для корректировки работы протокола штатными средствами, предусмотренными возможностями протокола BGP-4 и его реализациями на маршрутизаторах (такими как community, механизмы фильтрации принимаемой и анонсируемой маршрутной информации). Включение криптографических подписей требует существенной доработки алгоритма самого протокола BGP-4, что неизменно повлечет за собой отход от действующего стандарта и переход на новый.

Разработанный стандарт BGPsec [10–11] был утвержден в 2017 г и предлагает использование дополнительного атрибута BGPsec_PATH, который содержит цифровые подписи, подтверждающие подлинность происхождения маршрута-префикса и легитимность его распространения на всем пути. Подлинность маршрутов удостоверяется при помощи инфраструктуры открытых ключей — Resource Public Key Infrastructure (RPKI) [12], что является гибким решением, позволяющим контролировать не только достоверное происхождение маршрута, но и, например, максимальную длину допустимого для анонсирования маршрута-префикса (это позволит исключить неконтролируемое анонсирование более специфичных маршрутов). Однако, необходимым условием для внедрения BGPsec является способность маршрутизаторов АС поддерживать работу данного стандарта.

Данная работа ориентирована на развитие подхода, основанного на выявлении аномалий в маршрутной информации, с последующим применением готового рабочего решения в тандеме со стандартно эксплуатируемым протоколом BGP-4 на маршрутизаторах АС транзитного оператора. Предлагаемое решение позволит оперативно устанавливать факт появления аномальной маршрутной информации и корректировать работу маршрутизаторов транзитной АС, тем самым предотвращая дальнейшую дестабилизацию маршрутных таблиц и общей картины сетевой связности.

## Описание предлагаемого решения

Предлагаемое решение ориентировано на контроль текущей маршрутной информации, распространяемой при помощи протокола BGP-4, и выявления аномалий в обрабатываемой маршрутной информации АС контролируемого оператора связи. При этом полагается, что оператор связи является транзитным, т.е. имеет определенное количество подключений к вышестоящим транзитным операторам связи (Uplink_1 … Uplink_N), равноправные «пиринговые» подключения к другим операторам связи (Peer_1 … Peer_K) и «клиентские» подключения (Customer_1 … Customer_P), с обменом маршрутной информацией по протоколу BGP-4 и получением полной маршрутной таблицы, включающей все анонсируемые маршруты-префиксы от всех АС операторов связи сети Интернет — «full-view» (рис. 1). Предлагаемое решение должно анализировать регулярные обновления маршрутной информации, поступающее внутрь контролируемой АС по всем имеющимся подключениям, для предотвращения «утечек» и «угонов» маршрутов, которые могут быть инициированы как «извне» (маршрутная информация получена от вышестоящих операторов), так и по «пиринговым» и клиентским подключениям (маршрутная информация получена от операторов связи и клиентов). Это позволит транзитной контролируемой АС исключить некорректную маршрутную информацию из своих маршрутных таблиц, пресечь распространение некорректной маршрутной информации и дальнейшей дестабилизации межсетевого взаимодействия.

Предлагаемое решение подключается к сети контролируемого оператора по протоколу BGP-4 в качестве внешнего участника (используется номер приватной АС 65501) и получает все обновления маршрутной информации, поступающие в контролируемую АС (рис. 2). Все получаемые обновления обрабатываются «Модулем обработки обновлений маршрутной информации», после чего обработанное обновление ставится в «Очередь обновлений». Эта очередь разбирается «Модулем анализа обновлений», который выполняет проверку каждого обновления в соответствии с информацией, получаемой из базы данных RADb (Routing Assets Database) [13]. Проверяются соответствие присутствующего в обновлении маршрута-префикса с аналогичным в базе данных

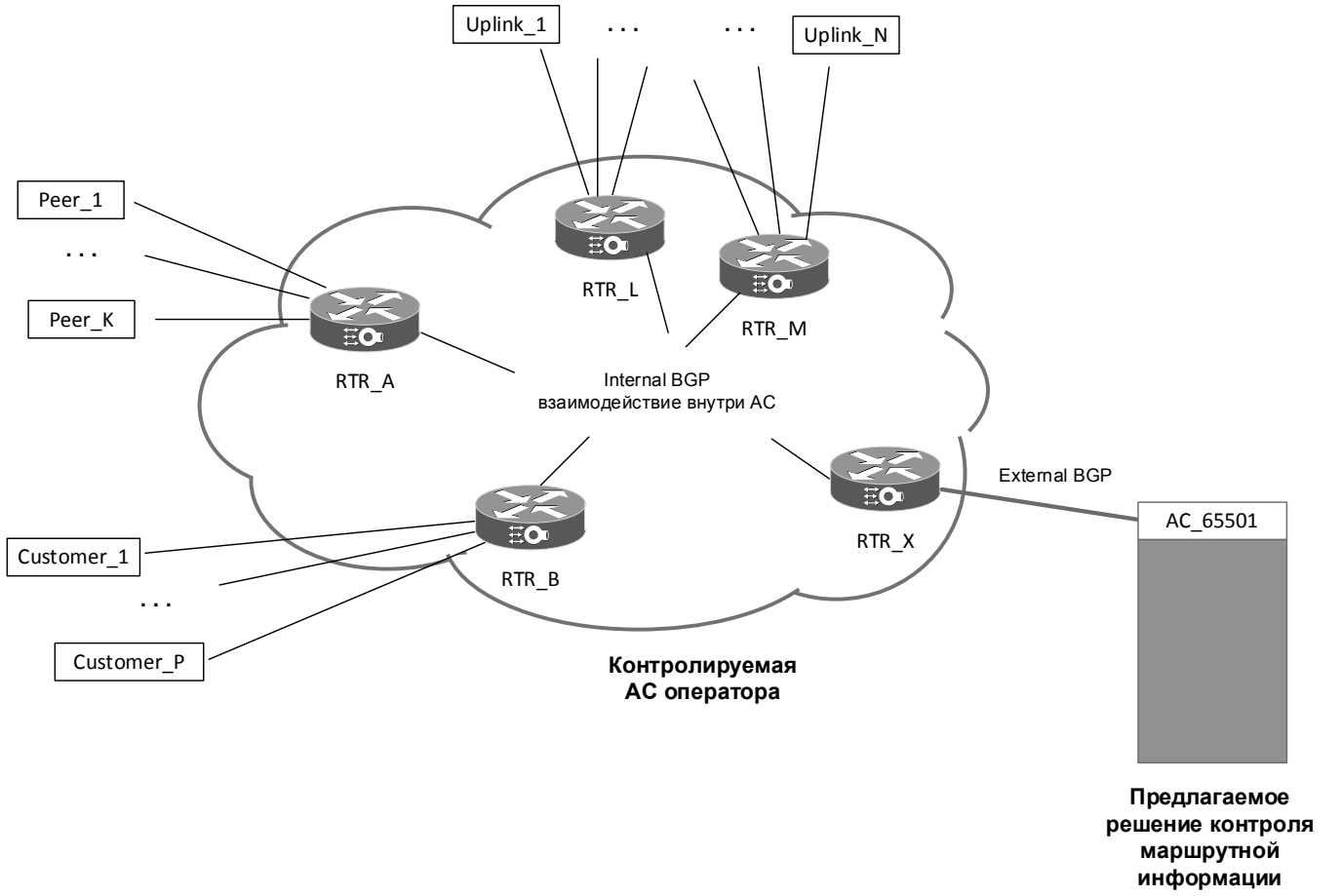


Рис. 1.Типовая схема межсетевого взаимодействия оператора связи и включение предлагаемого решения.

(БД) RADb, соответствие АС инициатора анонсируемого маршрута-префикса, легальность получения этого маршрута-префикса пограничным маршрутизатором контролируемой АС по одному из BGP-подключений. В случае обнаружения несоответствия формируется сообщения вида «Действие_М», которая ставится в «Очередь действий» для дальнейшей обработки «Модулями действий», которые формируют конечную реакцию — уведомление администратора, генерация фильтрующих листов для целевого маршрутизатора контролируемой АС, который получил конкретное аномальное обновление, и т.п. Для дополнительной информативности «Модуль анализа обновлений» может использовать информацию из других БД, входящих в список регистратур маршрутной информации сети Интернет — The Internet Routing Registry (IRR) [14] и поддерживающих RPSL (RFC2622) [15] или свой собственный язык описания объектов маршрутной информации. Наличие очередей в структуре предлагаемого решения позволяет рассинхронизировать процессы обработки и увеличить гибкость самого решения. Решение выполнено на языке программирования Python [16].

## Модуль обработки обновлений маршрутной информации

Модуль обработки обновлений маршрутной информации представляет собой «легкую» версию BGP-агента, способную устанавливать BGP-сессию с маршрутизатором и получать от него сообщения согласно спецификации протокола BGP-4 [1]. За основу был взят BGP-агент YABGP [17], выполненный на языке программирования Python.

Модуль подключается к BGP-маршрутизатору контролируемой АС, устанавливает BGP-сессию, выжидает начальный таймаут Time1 (чтобы пропустить первоначальную серию сообщений UPDATE — обновлений маршрутной информации от BGP-маршрутизатора контролируемой АС, когда маршрутизатор контролируемой АС одномоментно передает полное содержимое своей маршрутной таблицы) и, далее, начинает обрабатывать только приходящие UPDATE-сообщения (type = 2). Из UPDATE-сообщений выделяются такие атрибуты, как путь (AS_PATH), IP-адрес следующего маршрутизатора

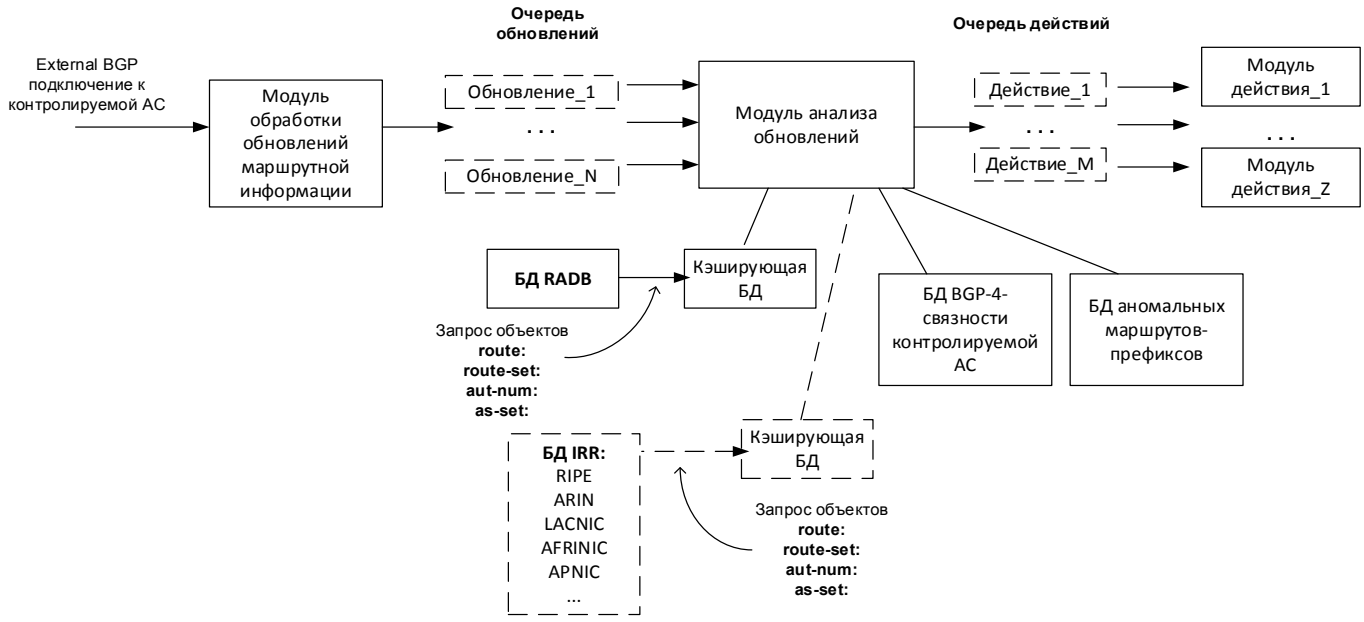


Рис. 2.Структурная схема предлагаемого решения.

(NEXT_HOP), анонсируемые маршруты (Network Layer Reachability Information — NLRI). Эти атрибуты формируют задание «Обновление_N», которое определяется в «Очередь обновлений». UPDATE-сообщения с отзываемыми маршрутами (Withdraw Message) игнорируются. Общий алгоритм работы модуля можно представить следующим образом:

**Подключение**(маршрутизатор контролируемой АС)
**Ожидание**(Time1)
**Для каждого**(Получаемое сообщение == UPDATE) **выполнить** {
  **Если** (Получаемое сообщение!= Withdraw message) **то** {
    Путь = Получаемое сообщение[AS_PATH]
    След_IP = Получаемое сообщение[NEXT_HOP]
    Маршруты = Получаемое сообщение[NLRI]
**Сформировать обновление и поставить в очередь**(Путь, След_IP, Маршруты)
  }
}

Модуль не совершает никаких предобработок извлеченной информации и способен быстро перейти к работе со следующим получаемым UPDATE-сообщением. Обработка иных BGP-сообщений и поддержание BGP-сессии осуществляется возможностями агента YABGP.

## Модуль анализа обновлений

Очередь обновлений циклично сканируется и обрабатывается «Модулем анализа обновлений». Каждое стоящее в очереди обновление передается на детальный анализ, в ходе которого выполняется следующее:

1. Запись «Путь» оптимизируется путем исключения многократно повторяющихся номеров одной и той же АС в общей цепочке, исключается номер контролируемой АС. В записи находится номер соседней с контролируемой АС (След_АС) и номер начальной АС (Нач_АС), являющейся источником маршрутной информации. Это необходимо для установления точки происхождения маршрутной информации, АС, от которой контролируемая АС получила данную маршрутную информацию, и общего пути распространения маршрутной информации.
2. В записи «Маршруты» выделяются все перечисленные маршруты-префиксы.
3. Маршруты-префиксы проверяются на совпадение с диапазонами приватных сетей [18]. Приватные сети не должны анонсироваться никаким оператором связи за пределы своей АС, в противном случае маршрут-префикс не проходит проверку.
4. Для каждого маршрута-префикса выполняется сравнение маршрута-префикса и номера начальной АС с информацией из БД RADb. Для этого из БД RADb запрашиваются объекты "**route**" и проводится сравнение маршрута-префикса с полем 'route:', номера начальной АС с полем 'origin:' запрошенного объекта. Любое расхождение (не соответствие маршрута-префикса и номера начальной АС с данными, полученными из БД) будет означать, что маршрут-префикс не прошел проверку.

5. Для всех АС, соседствующих с контролируемой АС и не являющихся вышестоящим транзитным оператором связи, выполняется иерархическая проверка объектов "**aut-num**" (поля 'import'), "**as-set**" и "**route-set**" (поля 'members') из БД RADb. Проверка заканчивается после нахождения номера начальной АС или проверяемого маршрута-префикса в содержимом указанных объектов. Этот этап необходим для подтверждения легальности пути распространения проверяемого маршрута-префикса.
6. Выполняется проверка на наличие маршрута-префикса в локальной «БД аномальных маршрутов-префиксов». Если не прошедший проверку маршрут-префикс отсутствует в указанной БД, то выполняется операция по внесению этого маршрута-префикса в «БД аномальных маршрутов-префиксов». Возможно, что не прошедший проверку маршрут-префикс уже был обработан ранее, в это случае такой маршрут-префикс уже содержится в указанной БД. В случае успешного прохождения проверки и наличия такого маршрута-префикса в БД происходит удаление маршрута-префикса из БД.

Для маршрутов-префиксов, не прошедших проверку, формируется «Действие_М» — специализированное уведомление, содержащее необходимую информацию для принятия дальнейших действий. Специализированное уведомление содержит:

- маршруты-префиксы из проанализированного «Обновления_N»;
- битовую переменную «Действие», биты которой, установленные в '1' будут определять идентификатор «Модуля действия» при их дальнейшей обработке;
- поля «Параметры_действия», которые включают в себя номер соседней с контролируемой АС (След_АС), а также набор информации из БД «BGP-4 связности контролируемой АС», позволяющей идентифицировать по IP-адресу маршрутизатор контролируемой АС, который получил по своей внешней BGP-сессии от соседней с контролируемой АС «След_АС» не прошедшие проверку маршруты-префиксы, название фильтрующего правила для входящей маршрутной информации от «След_АС» и прочие параметры, необходимые для осуществления запланированного действия.

Если маршрут-префикс прошел все предыдущие проверки, но при этом уже присутствует в «БД аномальных маршрутов-префиксов», то этот маршрут из БД удаляется, и происходит формирование специального уведомления для выполнения действия по отмене ранее принятых мер в отношении данного маршрута-префикса.

Алгоритм работы модуля приведен ниже и отражает основные моменты его функционирования:

```
Для каждого(Обновление_N(Путь, След_IP, Маршруты)) выполнить {
Путь, Нач_АС, След_АС = Оптимизировать и найти(Путь, контролируемая АС)
   Действие = 0
Тип_След_АС, Параметры_действия = Поиск в БД связности контролируемой АС(След_IP, След_АС)
  Для каждого (Маршрут_i из Маршруты)выполнить {
      Если (Маршрут_i Î Приватные сети) то {
  Установить(Действие, бит0 = 1)
  Сформировать уведомление(Маршрут_i, Действие, Параметры_действия)
  Поставить уведомление в очередь
  Продолжить цикл
}
Пр1 = Проверка начальной АС(Маршрут_i, Нач_АС)
Если (Пр1!= "Успешно") то {
  Установить(Действие, бит0 = 1)
  Установить(Действие, бит1 = 1)
}
Если (Тип_След_АС!= "Вышестоящий оператор") то {
Пр2 = Проверка пути (Маршрут_i, Нач_АС, След_АС)
  Если (Пр2!= "Успешно") то {
     Установить(Действие, бит1 = 1)
  }
}
Пр3 = Проверка в БД аномальных маршрутов (Маршрут_i)
Если (Пр3 == "Нет") И ((Действие, бит0 == 1) ИЛИ (Действие, бит1 == 1)) то {
  Внести в БД аномальных маршрутов(Маршрут_i)
} иначе Если (Пр3 == "Есть") И ((Действие, бит0 == 0) И (Действие, бит1 == 0)) то {
  Удалить из БД аномальных маршрутов(Маршрут_i)
  Установить(Действие, бит2 = 1)
}
Если (Действие!= 0) то {
Сформировать уведомление(Маршрут_i, Действие, Параметры_действия)
  Поставить уведомление в очередь
}
  }
}
```

Сформированное уведомление поступает в «Очередь действий» для их последующей обработки «Модулями действий». Для управления действиями использу-

ется битовое поле «Действие» в каждом уведомлении. Каждому биту соответствует свое действие, которое активизируется установкой бита в «1». На текущем этапе предусмотрены следующие действия:

Бит 0 — блокировка маршрута-префикса
Бит 1 — генерация предупреждающего сообщения
Бит 2 — разблокирование маршрута-префикса

Проверка маршрутов-префиксов и номеров АС осуществляется путем запроса требуемого объекта из БД RADb. В случае отсутствия в БД RADb запрашиваемого объекта запрос переадресуется в БД другого IRR — в данном случае, с учетом специфики обслуживания региона (и всей Российской Федерации в целом) — в БД регистратуры RIPE. Поддержка RPSL позволяет стандартизовать работу с запрошенными объектами и организовать иерархический запрос связанных объектов с поэтапной обработкой. В частности, при обработке объекта "**aut-num**" последовательно в соответствии с иерархией связей запрашиваются остальные объекты вида "**as-set**" и/или "**route-set**". Для снижения нагрузки на БД регистратур маршрутной информации все запрошенные объекты сохраняются в локальной кэширующей БД сроком на 24 часа, и повторно уже используются сохраненные в локальной кэширующей БД экземпляры объектов.

Обработка объектов "**aut-num**", "**as-set**" и "**route-set**" однозначно требует для всех BGP-соседей контролируемой АС (за исключением вышестоящих операторов связи) и связанных с ними нижестоящих АС ответственно относиться к своей политике маршрутизации и поддерживать свои собственные объекты, отражающие политику маршрутизации, в актуальном состоянии в БД IRR. Несоблюдение этого условия будет приводить к идентификации получаемых маршрутов-префиксов как аномальных. Для уменьшения строгости действий, принимаемых по итогам неудачной проверки пути распространения маршрута-префикса после анализа объектов, блокирования маршрута-префикса в данный момент не производится, но генерируется предупреждающее сообщение.

БД «BGP-4 связности контролируемой АС» хранит основную информацию о топологии и взаимоотношениях BGP-маршрутизаторов контролируемой АС. Помимо идентификатора маршрутизатора, его IP-адреса(ов) также ведется перечень всех внешних BGP-соседей каждого маршрутизатора с указанием модели маршрутизатора (например, Cisco, Juniper, …), типа BGP-соседа (например, «вышестоящий оператор», «пиринг», «клиент», …), названия применяемого списка фильтрации для входящих маршрутов, контактная информация администраторов контролируемой АС и соседних АС, дополнительная информация об особенностях работы с конкретным маршрутизатором при осуществлении с ним определенных действий.

В качестве локальных БД используется документоориентированная БД mongoDB [19], которая позволяет эффективно осуществлять поиск и выборку требуемой информации по сохраненным объектам БД IRR и среди информации, описывающей топологию и связность BGP-маршрутизаторов контролируемой АС.

## Модули действий

«Очередь действий» обрабатывается модулями действий. Каждый из модулей действия проверяет соответствующий ему бит в битовой переменной «Действие», содержащейся внутри каждого уведомления в «Очереди действий». После обработки уведомления из очереди каждый модуль обнуляет соответствующий ему бит.

В соответствии с определенными для каждого действия бита на текущем этапе очередь обрабатывается тремя модулями действий:

1. Модуль блокировки — (бит 0) — выполняет внесение маршрута-префикса из уведомления в список фильтрации входящих маршрутов для BGP-соседа с номером «След_АС», обновление списка фильтрации на соответствующем BGP-маршрутизаторе контролируемой АС и переконфигурацию BGP-сессии со «След_АС» для применения сделанных изменений.
2. Модуль предупреждения — (бит 1) — генерирует предупреждающее сообщение о маршруте-префиксе, которое отправляется на контактные данные администратора контролируемой АС и, при необходимости, на контактные данные администратора соседней АС с номером «След_АС».
3. Модуль разблокировки — (бит 2) — функционально аналогичен Модулю блокировки, но выполняет процесс разблокирования маршрута-префикса — т.е. его удаление из списка фильтрации.

Количество действий определяется количеством используемых битов переменной «Действие». При необходимости, перечень действий может быть легко расширен путем добавления новых битов и включения нового модуля действия в число анализирующих «Очередь действий». Соответственно, для этого необходимо выполнить доработку «Модуля анализа обновлений».

## Заключение

В работе предлагается вариант решения для контроля текущей маршрутной информации, распространяемой при помощи протокола BGP-4, и выявления аномалий в обрабатываемой маршрутной информации.

Данное решение не требует модификации действующего программного обеспечения BGP-маршрутизаторов и поддержки современных модификаций протокола BGP-4. Дальнейшая работа ориентирована на оптимизацию работы модулей предлагаемого решения, учет большего количества возможных ситуаций, связанных с распространением и обработкой маршрутной информации, а также адаптирование предлагаемого решения для более сложных топологий и способов взаимодействия маршрутизаторов внутри контролируемой АС.

ЛИТЕРАТУРА


1. Y. Rekhter, T. Li, S. Hares. RFC4271 — A Border Gateway Protocol 4 (BGP-4). [Электронный ресурс] — Режим доступа — URL: https://tools.ietf.org/html/rfc4271 (дата обращения 25.06.2019)
2. K. Butler, T. Farley, P. McDaniel, J. Rexford. A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE. 2009. V. 98, I.1, pp. 100–122. DOI: 10.1109/JPROC.2009.2034031
3. Q. Li, J. Liu, Y. Hu, M. Xu, J. Wu. BGP with BGPsec: Attacks and Countermeasures. IEEE Network. 2018. pp. 1–7. DOI: 10.1109/MNET.2018.1800171
4. BGPMon / BGPStream. [Электронный ресурс] — Режим доступа — URL: https://bgpstream.com/ (дата обращения 25.06.2019)
5. J. M. Smith, K. Birkeland, M. Schuchard. An Internet-Scale Feasibility Study of BGP Poisoning as a Security Primitive. 2018. DOI: arXiv:1811.03716v5 [cs.CR]
6. G. Huston, M. Rossi, G. Armitage. Securing BGP — A Literature Survey. IEEE Communications Surveys & Tutorials. 2011. V. 13(2), pp. 199–222. DOI: 10.1109/SURV.2011.041010.00041
7. R. Hiran, N. Carlsson, N. Shahmehri. Does scale, size, and locality matter? Evaluation of collaborative BGP security mechanisms. Proc. IFIP Networking, 2016. pp. 261–269. DOI: 10.1109/IFIPNetworking.2016.7497237.
8. S. Kent, Ch. Lynn, K. Seo. Secure border gateway protocol (S-BGP). IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. 2000. V. 18(4). pp. 582–592. DOI: 10.1109/49.839934.
9. M. Zhao, S. W. Smith, D. M. Nicol. The performance impact of BGP security. IEEE Network. 2005. V. 19(6). pp. 42–48. DOI: 10.1109/MNET.2005.1541720
10. M. Lepinski, K. Sriram. RFC8205 — BGPsec Protocol Specification. [Электронный ресурс] — Режим доступа — URL: https://tools.ietf.org/html/rfc8205 (дата обращения 25.06.2019)
11. W. George, S. Murphy. RFC8206 — BGPsec Considerations for Autonomous System (AS) Migration. [Электронный ресурс] — Режим доступа — URL: https://tools.ietf.org/html/rfc8206 (дата обращения 25.06.2019)
12. M. Lepinski, S. Kent. RFC6480 — An Infrastructure to Support Secure Internet Routing. [Электронный ресурс] — Режим доступа — URL: https://tools.ietf.org/html/rfc8206 (дата обращения 25.06.2019)
13. The Internet Routing Registry — RADb. [Электронный ресурс] — Режим доступа — URL: https://www.radb.net/ (дата обращения 25.06.2019)
14. List of Routing Registries — The Internet Routing Registry (IRR). [Электронный ресурс] — Режим доступа — URL: http://www.irr.net/docs/list.html (дата обращения 25.06.2019)
15. Routing Policy Specification Language (RPSL). [Электронный ресурс] — Режим доступа — URL: https://tools.ietf.org/html/rfc2622 (дата обращения 25.06.2019)
16. Python. [Электронный ресурс] — Режим доступа — URL: https://www.python.org/ (дата обращения 25.06.2019)
17. YABGP Project. [Электронный ресурс] — Режим доступа — URL: https://yabgp.readthedocs.io/en/latest/ (дата обращения 25.06.2019)
18. Address Allocation for Private Internets. [Электронный ресурс] — Режим доступа — URL: https://tools.ietf.org/html/rfc1918 (дата обращения 25.06.2019)
19. mongoDB. [Электронный ресурс] — Режим доступа — URL: https://www.mongodb.com/ (дата обращения 25.06.2019)




Журнал «Современная наука: актуальные проблемы теории и практики»