**УДК 343.3/7** **DOI: 10.34670/AR.2022.48.65.019**

# Нарушение маршрутизации компьютерной информации: концепция нового состава преступления для России

**Олифиренко Артем Алексеевич**

Студент,
Саратовская государственная юридическая академия,
410056, Российская Федерация, Саратов, ул. Вольская, 1;
e-mail: panolifer@gmail.com

**Аннотация**

С каждым годом сотрудникам правоохранительных органов становится все труднее выявлять и пресекать киберпреступления, однако даже то, что недавно не представляло серьезной опасности, теперь является одним из серьезных преступлений. Перехват протокола автономной межсистемной (AS) маршрутизации (BGP hijacking) – это киберугроза не только для России, но и для всех стран. Данное исследование доказывает, что нарушение маршрутизации компьютерной информации должно стать новым составом преступления в Уголовном кодексе РФ в главе преступлений в сфере компьютерной информации. Поскольку целью преступника является не осуществление процесса модификации самой информации, а сохранение ее в измененном виде в источнике информации с использованием алгоритмов маршрутизации данных (информации), пока кто-нибудь не заметит и не исправит маршрутизацию, трафик IP-адреса будет перенаправляться на AS злоумышленника, что не подпадает под современный Уголовный кодекс РФ, предлагаются соответствующие поправки в главу 28 (ст. 272, 273, 274, 271[1]) для улучшения уголовной законодательной базы в части противостояния и противодействия киберпреступлениям.

**Для цитирования в научных исследованиях**

Олифиренко А.А. Нарушение маршрутизации компьютерной информации: концепция нового состава преступления для России // Вопросы российского и международного права. 2021. Том 11. № 12А. С. 187-194. DOI: 10.34670/AR.2022.48.65.019

**Ключевые слова**

Перехват маршрута, маршрутизация данных, состав преступления, киберпреступность, Россия.

## Введение

Мир находится в Сети, как и преступники. Соответственно, киберпреступность – это не что иное, как любая незаконная деятельность, осуществляемая с использованием информационных технологий. Киберпреступники взламывают персональные компьютеры, смартфоны, личные данные из социальных сетей, коммерческие секреты, государственные секреты, важные личные данные и т. д., используя Интернет и компьютерные устройства. За последние несколько десятилетий мы продолжили стремительную цифровую трансформацию. Растущие киберугрозы могут стать вознаграждением за эффективность, которую мы получили от перехода к цифровым технологиям. Несколько IT-систем были разработаны и использованы без должного внимания к безопасности. Кроме того, со временем обнаруживаются новые уязвимости в системе безопасности. Этот вопрос следует считать важным, поскольку защита от киберугроз стала основной функцией государства, а не отдельной службы или предприятия. Преступления в сфере компьютерной информации в современный период технологического и информационного прогресса приобретают масштабные проявления, наполняются новыми признаками, которые с учетом законодательного регулирования данной сферы общественных отношений требуют совершенствования нормативных предписаний [Csonka, 2000].

Состав преступлений, предусмотренных ст. 272 и 274 УК РФ, материальный, что требует наступления последствий в виде уничтожения, блокирования, модификации или копирования компьютерной информации.

## Основная часть

Появились новые способы обхода как компьютерной защиты, так и уголовного законодательства в сфере компьютерной информации. Таковым является нарушение маршрутизации данных. Конечно, можно говорить, что, взламывая код государственного сайта, преступник модифицирует информацию, хранящуюся в бэкенде сайта (серверная часть сайта, где заключается программно-аппаратный раздел, способствующий функционированию фронтенда – клиентской части сайта). Однако представляется, что модификацию информации в данном случае следует рассматривать не как сам процесс внесения изменений в нее, а как результат этого процесса, т. е. как сохранение информации в измененном виде.

Нарушение маршрутизации комьютерной информации – это способ просмотра потенциально конфиденциальной информации – от финансовых транзакций до правительственных документов. Все это возможно благодаря протоколам, работающим в глобальном Интернете, которые не созданы с учетом строгой безопасности.

При совершении преступного посягательства, направленного на сохранность компьютерной информации, целью преступника является не осуществление самого процесса модификации информации, а сохранение ее в измененном виде в источнике информации с использованием алгоритмов маршрутизации данных (информации), что не подпадает под современную квалификацию дел по главе 28 УК РФ. Это совершенно иной подход к хакингу: по сути, нет нейтрализации средств защиты компьютерной информации[1]. Это тип атаки, который по-английски называется hijacking, но в нашем случае нужна еще и приписка BGP (протокол

[1] См. Постановление Московского городского суда от 13 декабря 2013 г. № 4у/9-9343/13.

автономной межсистемной (AS) маршрутизации, созданный для использования на основных интернет-маршрутизаторах, с помощью которого сеть в Интернете сообщает о факте своего существования и о том, к каким сетям можно подключиться через них). С полученным трафиком злоумышленник может делать что угодно, например анализировать на предмет определенной информации так, чтобы в источнике информации она сохранилась в измененном виде и была возвращена в Сеть, что согласовывается с требованиями ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ, где доступ к информации понимается как возможность ее получения и использования, значит, это и есть преступление.

Более четкая идентификация, в соответствии с которой программные продукты (модули) могут быть классифицированы как вредоносные, еще не предусмотрена, не установлена законом и не разработана судебной практикой. Для того чтобы заявление о вредоносном ПО имело юридическую силу, необходимо провести программно-техническое расследование в соответствии со всеми правилами, установленными в уголовном производстве. Однако в данном случае нарушение маршрутизации компьютерной информации не уничтожает, не блокирует, не модифицирует и не копирует информацию: оно незаметно маскируется и получает доступ к информации, которая уже будет сохраняться в измененном виде.

Процесс, посредством которого устройства в разных сетях определяют, как они взаимодействуют друг с другом, называется маршрутизацией. Маршрутизация обычно выполняется на устройствах, называемых маршрутизаторами. Они перенаправляют сетевые «пакеты» между узлами сети, используя таблицу маршрутизации, пока они не достигнут конечного пункта назначения. В общем случае маршрутизация может выполняться не только маршрутизаторами, но и обычными операционными системами, установленными на рабочих компьютерах [Продвинутое туннелирование…, www].

Интернет-маршрутизаторы развертываются и управляются различными административными подразделениями, называемыми автономными системами (AS представляет собой набор компьютерных сетей IP, интегрированных в Интернет, чья внутренняя политика маршрутизации (маршруты, которые должны быть выбраны в первую очередь, фильтрация объявлений) согласована). В своей сети AS может выбрать протокол маршрутизации и показатели по своему усмотрению. Маршрутизация между различными сетями AS (междоменная маршрутизация) использует протокол пограничного шлюза (BGP представляет собой протокол, с помощью которого информация о маршрутизации обменивается между автономными системами) [Giotsas, Zhou, www].

BGP – это единственный протокол маршрутизации, который использует TCP в качестве своего транспортного протокола. Маршрутизаторы, получившие информацию BGP, выбирают наилучший маршрут к сети назначения и добавляют его в свои таблицы маршрутизации. BGP использует различные параметры для определения наилучшего маршрута. Наиболее очевидным из них является количество сетей до пункта назначения – длина так называемого пути оси. Чем короче путь оси, тем выгоднее маршрут [Сети…, www].

Соседние маршрутизаторы идентифицируются по их идентификатору маршрутизатора [Chen, Yuan, www], четырехбайтовому идентификатору, уникальному для каждого из маршрутизаторов данной автономной системы (AS), который может быть выбран произвольно, но который, как правило, представляет собой петлю IPV41011, 12, 13, 14 адреса каждого маршрутизатора.

Существует два режима работы BGP: внутренний BGP (iBGP) и внешний BGP (eBGP). iBGP используется внутри автономной системы, в то время как eBGP используется между двумя AS.

Как правило, соединения eBGP устанавливаются по двухточечным соединениям или в локальных сетях (например, точка обмена данными в Интернете), затем TTL пакетов сеанса BGP устанавливается равным [Harrington, 2003]. Если физическая связь разорвана, то же самое происходит и с сеансом eBGP и все префиксы, изученные им, объявляются удаленными и удаляются из таблицы маршрутизации.

Соединения iBGP обычно устанавливаются между логическими IP-адресами, не связанными с конкретным физическим интерфейсом (адреса обратной связи). Обычно используется протокол динамической внутренней маршрутизации (IGP) [BGP fundamentals, www] (в общем случае OSPF или IS-IS), который позволяет маршрутизаторам рассматриваемой сети подключаться через их адреса обратной связи [Smith, www]. Таким образом, в случае разрыва физической связи сеанс iBGP остается активным [Osterloh, 2001], если существует альтернативная связь.

Как только соединение между двумя маршрутизаторами установлено, они обмениваются информацией о сетях, которые они знают и для которых они предлагают транзит, а также о ряде атрибутов, связанных с этими сетями, которые позволят избежать петель (таких как путь) и тонко выбрать лучший маршрут.

В протоколе BGP отсутствует аутентичный механизм для аутентификации маршрутов, что приводит к уязвимости, при которой любой маршрутизатор BGP может объявить любой префикс, как если бы у него был этот префикс, или даже изменить маршрут, связанный с префиксом. Большинство сетевых операторов настраивают маршрутизаторы BGP для установления одноранговых отношений с другими автономными системами с целью обмена информацией о маршрутизации. Однако они не имеют никакого контроля над тем, кто допущен в BGP. Кроме того, сам протокол BGP имеет необходимые механизмы для проверки владения префиксом (или пути к определенному префиксу). Вредоносный объект может захватить префиксы других автономных систем, подвергая опасности маршрутизатор, говорящий по протоколу BGP, или участвуя в самой глобальной маршрутизации. В некоторых случаях перехваты BGP происходят из-за неправильных настроек [What…, www].

Но как происходит процесс хаккинга в таком случае? Когда AS объявляет маршрут к IP-префиксам, которые она фактически не контролирует, это объявление, если оно не отфильтровано, может распространяться и добавляться в таблицы маршрутизации в маршрутизаторах BGP через Интернет. Пока кто-нибудь не заметит и не исправит маршруты, трафик на эти IP-адреса будет перенаправляться на эту AS [BGP hijacking, www].

Концепция взлома BGP основана на поиске провайдера, который не фильтрует рекламу (намеренно или иным образом), или на поиске провайдера, внутренний сеанс BGP или сеанс BGP между провайдерами которого подвержен атаке хакера в данном контексте – «человек посередине» (это форма атаки, при которой данные, которыми обмениваются две стороны, каким-то образом перехватываются, записываются и, возможно, изменяются злоумышленником без ведома жертв; при обычном общении два задействованных элемента взаимодействуют друг с другом без помех через среду, локальную сеть в Интернете или и то и другое) [Aziz, Hamilton, www]. После обнаружения злоумышленник потенциально может объявить любой префикс, который он хочет, в результате чего часть или весь трафик будет перенаправлен от реального источника к злоумышленнику. Это может быть сделано либо для перегрузки интернет-провайдера, в который проник злоумышленник, либо для выполнения атаки DOS, либо для олицетворения на объект, префикс которого объявляется. Нередко злоумышленник вызывает серьезные сбои, вплоть до полной потери подключения.

Злоумышленник успешно маскируется под одного из участников сеанса BGP и требует той же информации, что есть у всех участников сеанса. Она может быть направлена на достижение большего, чем просто отключение сеанса между одноранговыми (одноуровневыми) узлами BGP. Например, целью может быть изменение маршрутов, используемых одноранговым узлом, для облегчения подслушивания, поиска «черных дыр» или анализа трафика. Примечательно, что примеры BGP hijacking можно встретить даже на github (например, работа итальянского программиста под ником «mastinux» [BGP path hijacking attack, www]).

Чтобы ограничить перехват BGP, предлагался большой пласт методов обнаружения. Во-первых, это возможно путем поиска нарушения AS множественного происхождения (MOAS – мы используем двоичную цифру для обозначения конфликта MOAS, что является одним из стандартных правил для определения перехвата BGP), нарушения политики BGP, отслеживания того, появляются ли внезапно новые пары соседних AS [Karlin, Forrest, Rexford, www]. Во-вторых, можно измерять количество атак с захватом путем сопоставления нескольких источников информации с поверхностей данных и управления сетью и поиска несоответствий между ними или проверки ее доступности [Shi et al., www]. В-третьих, можно использовать тесты ping для обнаружения подобных атак [Tahara et al., 2008].

Были предприняты значительные усилия по повышению безопасности BGP. В настоящее время наиболее распространенным приемом является использование входных (входящих) фильтров, построенных на данных реестров интернет-маршрутизации (IRR представляет собой базу данных объектов интернет-маршрутов для определения и совместного использования маршрута и соответствующей информации, используемой для настройки маршрутизаторов, чтобы избежать проблемных вопросов между интернет-провайдерами). Идея проста: используйте «одобренные» объекты маршрута и наборы осей для создания фильтров для ссылок клиентов. Основная проблема заключается в том, что как активы, так и объекты маршрута отличаются от одного потока к другому и иногда разные объекты могут существовать с одним и тем же идентификатором в отдельных IRR. Конечно же, политика IRR не является обязательной: она является добровольной для реализации, что приводит нас к ситуации, когда многие из IPv4 (основаны на модели наилучших усилий, которая не гарантирует ни доставку, ни предотвращение двойной доставки и поддерживается транспортным протоколом верхнего уровня, таким как Протокол управления передачей (TCP) [IPv4…, www]) и IPv6 (предлагает адрес в 128 бит или 16 байт, что делает набор адресов около 340 триллионов триллионов (undecilion); он значительно больше, чем размер адреса, предоставляемого IPv4, поскольку состоит из восьми групп символов длиной 16 бит; большой размер подчеркивает, почему сети должны как можно скорее перейти на IPv6 [Ibidem]) не имеют зарегистрированных объектов или имеют их неправильно. Много объектов IRR плохо обслуживаются, и даже некоторые крупные сети уровня 2 не могут правильно настроить свои фильтры [Eliminating…, www].

Злоумышленник успешно маскируется под одного из участников сеанса BGP и требует той же информации, необходимой для выполнения атаки сброса. Разница в том, что атака с захватом сеанса может быть направлена на достижение большего, чем просто отключение сеанса между одноранговыми узлами BGP. Например, целью может быть изменение маршрутов, используемых одноранговым узлом, для облегчения подслушивания, поиска «черных дыр» или анализа трафика.

Анализ содержания маршрутизации информации позволяет заключить, что она является самостоятельным явлением, не входящим в модификацию информации.

Таким образом, предлагается в составы преступлений УК РФ внести следующие

дополнения:

– в ст. 272 УК РФ включить последствие «если это деяние повлекло… нарушение маршрутизации компьютерной информации»;
– в ст. 274 УК РФ включить последствие «повлекшее… нарушение маршрутизации компьютерной информации»;
– в ст. 273 УК РФ включить предмет преступления при создании, распространении или использовании «компьютерных программ либо иной компьютерной информации, заведомо предназначенных для… нарушения маршрутизации информации»;
– в ст. 274[1] УК РФ включить предмет преступления при создании, распространении и (или) использовании «компьютерных программ либо иной компьютерной информации, заведомо предназначенных для… нарушения маршрутизации информации».

## Заключение

Состав преступления, предусмотренный ст. 272 УК РФ (а также ст. 274 УК РФ), является материальным. В конструкцию его объективной стороны входят преступное деяние в форме действия либо бездействия и преступное последствие, а также причинная связь между ними, причем нарушение маршрутизации информации должно выступать признаком последствия этих преступлений. Составы ст. 273 и 274.1 УК РФ не требуют наступления последствий, в них маршрутизация информации должна выступать предметом преступления в сочетании с компьютерными программой и (или) информацией.

## Библиография

1. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27.07.2006 № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 08.07.2006: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14.07.2006. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/
2. Продвинутое туннелирование: атакуем внутренние узлы корпоративной сети. URL: https://habr.com/ru/post/326148/
3. Сети для самых маленьких. Часть восьмая. BGP и IP SLA. URL: https://habr.com/ru/post/184350/
4. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24.05.1996: одобр. Советом Федерации Федер. Собр. Рос. Федерации 05.06.1996. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
5. Aziz B., Hamilton G. Detecting man-in-the-middle attacks by precise timing. URL: https://ieeexplore.ieee.org/document/5211025
6. BGP fundamentals. URL: https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=7
7. BGP hijacking. URL: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/
8. BGP path hijacking attack. URL: https://github.com/mastinux/bgp-path-hijacking-attack
9. Chen E., Yuan J. Autonomous-system-wide unique BGP identifier for BGP-4. URL: https://datatracker.ietf.org/doc/html/rfc6286
10. Csonka P. The draft Council of Europe Convention on cybercrime: a response to the challenge of crime in the age of the internet? // Computer law and security report. 2000. Vol. 16. No. 5. P. 329-330.
11. Eliminating opportunities for traffic hijacking. URL: https://habr.com/ru/company/qrator/blog/442264/
12. Giotsas V., Zhou S. Valley-free violation in Internet routing – analysis based on BGP Community data. URL: https://www.researchgate.net/publication/261204878_Valley-free_violation_in_Internet_routing_-_Analysis_based_on_BGP_Community_data
13. Harrington D.L. CCNP practical studies: troubleshooting. Cisco Press, 2003. 820 p.
14. IPv4 vs IPv6: understanding the differences and looking ahead. URL: https://phoenixnap.com/blog/ipv4-vs-ipv6
15. Karlin J., Forrest S., Rexford J. Pretty good BGP: improving BGP by cautiously adopting routes. URL: https://www.cs.princeton.edu/~jrex/papers/pgbgp.pdf
16. Osterloh H. IP routing primer plus. Sams Publishing, 2001. 504 p.
17. Shi X., Xiang Y., Wang Z., Yin X., Wu J. Detecting prefix hijackings in the internet with argus. URL:

https://dl.acm.org/doi/10.1145/2398776.2398779
18. Smith P. BGP best practices. URL: https://www.ripe.net/participate/meetings/regional-meetings/manama-2006/BGPBCP.pdf
19. Tahara M., Tateishi N., Oimatsu T., Majima S. A method to detectprefix hijacking by using ping tests // Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management. Beijing, 2008. P. 390-398.
20. What is BGP hijacking? URL: https://www.psychz.net/client/question/en/what-is-bgp-hijacking.html

# BGP hijacking: the concept of a new corpus delicti for Russia

**Artem A. Olifirenko**

Student,
Saratov State Law Academy,
410056, 1 Volskaya str., Saratov, Russian Federation;
e-mail: panolifer@gmail.com

**Abstract**

The article deals with BGP hijacking. The author of the article points out that it is difficult for law enforcement officers to detect and stop cybercrimes. However, even what recently did not pose a serious danger is now one of the serious crimes. BGP hijacking is a cyber threat not only to Russia, but also to all countries. This study proves that BGP hijacking should become a new crime in the Criminal Code of the Russian Federation in the chapter of crimes in the field of computer information. The purpose of a criminal is not to carry out the process of modifying information itself, but to save it in a modified form in the source of information using data (information) routing algorithms, until someone notices and corrects the routing, IP address traffic will be redirected to the attacker's autonomous system, which does not fall under the modern Criminal Code of the Russian Federation. Having considered BGP hijacking as a possible corpus delicti for Russia, the author proposes to make the appropriate amendments to Chapter 28 of the Criminal Code of the Russian Federation (Articles 272, 273, 274, $271^1$) in order to improve the criminal legal framework in terms of countering cybercrime.

**For citation**

Olifirenko A.A. (2021) Narushenie marshrutizatsii komp'yuternoi informatsii: kontseptsiya novogo sostava prestupleniya dlya Rossii [BGP hijacking: the concept of a new corpus delicti for Russia]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 11 (12A), pp. 187-194. DOI: 10.34670/AR.2022.48.65.019

**Keywords**

BGP hijacking, data routing, corpus delicti, cybercrime, Russia.

## References

1. Aziz B., Hamilton G. *Detecting man-in-the-middle attacks by precise timing*. Available at: https://ieeexplore.ieee.org/document/5211025 [Accessed 27/11/21].
2. *BGP fundamentals*. Available at: https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=7 [Accessed 27/11/21].
3. *BGP hijacking*. Available at: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/ [Accessed

27/11/21].
4. *BGP path hijacking attack*. Available at: https://github.com/mastinux/bgp-path-hijacking-attack [Accessed 27/11/21].
5. Chen E., Yuan J. *Autonomous-system-wide unique BGP identifier for BGP-4*. Available at: https://datatracker.ietf.org/doc/html/rfc6286 [Accessed 27/11/21].
6. Csonka P. (2000) The draft Council of Europe Convention on cybercrime: a response to the challenge of crime in the age of the internet? *Computer law and security report*, 16 (5), pp. 329-330.
7. *Eliminating opportunities for traffic hijacking*. Available at: https://habr.com/ru/company/qrator/blog/442264/ [Accessed 27/11/21].
8. Giotsas V., Zhou S. *Valley-free violation in Internet routing – analysis based on BGP Community data*. Available at: https://www.researchgate.net/publication/261204878_Valley-free_violation_in_Internet_routing_-_Analysis_based_on_BGP_Community_data [Accessed 27/11/21].
9. Harrington D.L. (2003) *CCNP practical studies: troubleshooting*. Cisco Press.
10. *IPv4 vs IPv6: understanding the differences and looking ahead*. Available at: https://phoenixnap.com/blog/ipv4-vs-ipv6 [Accessed 27/11/21].
11. Karlin J., Forrest S., Rexford J. *Pretty good BGP: improving BGP by cautiously adopting routes*. Available at: https://www.cs.princeton.edu/~jrex/papers/pgbgp.pdf [Accessed 27/11/21].
12. *Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: feder. zakon Ros. Federatsii ot 27.07.2006 № 149-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 08.07.2006: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 14.07.2006* [On information, information technology and on information protection: Federal Law of the Russian Federation No. 149-FZ of July 27, 2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61798/ [Accessed 27/11/21].
13. Osterloh H. (2001) *IP routing primer plus*. Sams Publishing.
14. *Prodvinutoe tunnelirovanie: atakuem vnutrennie uzly korporativnoi seti* [Advanced tunneling: attacking the internal nodes of the corporate network]. Available at: https://habr.com/ru/post/326148/ [Accessed 27/11/21].
15. *Seti dlya samykh malen'kikh. Chast' vos'maya. BGP i IP SLA* [Networks for the youngest. Part eight. BGP and IP SLA]. Available at: https://habr.com/ru/post/184350/ [Accessed 27/11/21].
16. Shi X., Xiang Y., Wang Z., Yin X., Wu J. *Detecting prefix hijackings in the internet with argus*. Available at: https://dl.acm.org/doi/10.1145/2398776.2398779 [Accessed 27/11/21].
17. Smith P. *BGP best practices*. Available at: https://www.ripe.net/participate/meetings/regional-meetings/manama-2006/BGPBCP.pdf [Accessed 27/11/21].
18. Tahara M., Tateishi N., Oimatsu T., Majima S. (2008) A method to detectprefix hijacking by using ping tests. *Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management*. Beijing, pp. 390-398.
19. *Ugolovnyi kodeks Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 13.06.1996 № 63-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 24.05.1996: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 05.06.1996* [Criminal Code of the Russian Federation: Federal Law of the Russian Federation No. 63-FZ of June 13, 1996]. Available at: http://www.consultant.ru/document/cons_doc_LAW_10699/ [Accessed 27/11/21].
20. *What is BGP hijacking?* Available at: https://www.psychz.net/client/question/en/what-is-bgp-hijacking.html [Accessed 27/11/21].