*Д. А. Мельников, А. В. Неваленный, А. В. Соболева, Р. И. Смолокуров, А. Д. Мельников*

# К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ СВОЙСТВ ЛОГИЧЕСКОЙ ХАРАКТЕРИСТИКИ IPV6-ПРОТОКОЛА В ЦЕЛЯХ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ[1]

## Предисловие

Ежегодно в Интернет-сети наблюдается постоянный рост киберпреступлений. Только в 2012 г. ущерб от киберпреступности был оценён в $2 миллиарда в России и в $110 миллиардов во всем мире [1]. Цифры говорят сами за себя. При этом выявление самих киберпреступников остаётся весьма сложной задачей, решение которой в большинстве случаев найти невозможно. В данной статье предлагается способ, который может снизить остроту этой проблемы на основе использования логической характеристики IPv6-протокола (RFC-2460 и RFC-4291 [2,3]) и стандарта ISO 3166 [4]. А при условии неотвратимости наказания за киберпреступления, в перспективе, можно решить проблему обеспечения информационной безопасности (ИБ) государства и всего мирового сообщества.

| *n бит* | *m бит* | *128-n-m бит* |
|---|---|---|
| Префикс глобальной маршрутизации | Идентификатор подсети | Идентификатор интерфейса |

*Рис. 1. Общий формат глобального однонаправленного IPv6-адреса*

## Предпосылки

**Предпосылка первая**. В Интернет-сообществе обострилась проблема нехватки IP-адресов 4-й версии (IPv4), длина которых составляет 32 бита. В конце 90-х годов прошлого века была предложена система IP-адресации 6-ой версии (IPv6) [2,3], которая определила 128-битовую длину адреса. Общая ёмкость IPv6-адресного пространства составляет: $2^{128} \approx 10^{39}$. Это число IPv6-адресов во много раз превышает численность населения Земли.

Стандарты [2,3] определяют формат кодирования глобального однонаправленного (*unicast*) IPv6-адреса, который представлен на рис. 1.

Префикс глобальной маршрутизации присваивается группе подсетей (линий связи), а идентификатор подсети присваивается линии связи в рамках этой группы подсетей. Все глобальные однонаправленные IPv6-адреса имеют 64-битовой поле «Идентификатор интерфейса» (то есть, $n + m = 64$).

**Предпосылка вторая**. Международная организация по стандартизации (ISO) приняла в 1974 году первую версию Международного стандарта ISO 3166 [4], определяющего кодовые обозначения государств и зависимых территорий, а также основных административных образований внутри государств. Таким образом, каждая страна «получила» цифровое обозначение, состоящее из трёх цифр, например, Россия – 643, США – 840.

[1] Данная работа выполнена в НИЯУ МИФИ и МГУЭСИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050.

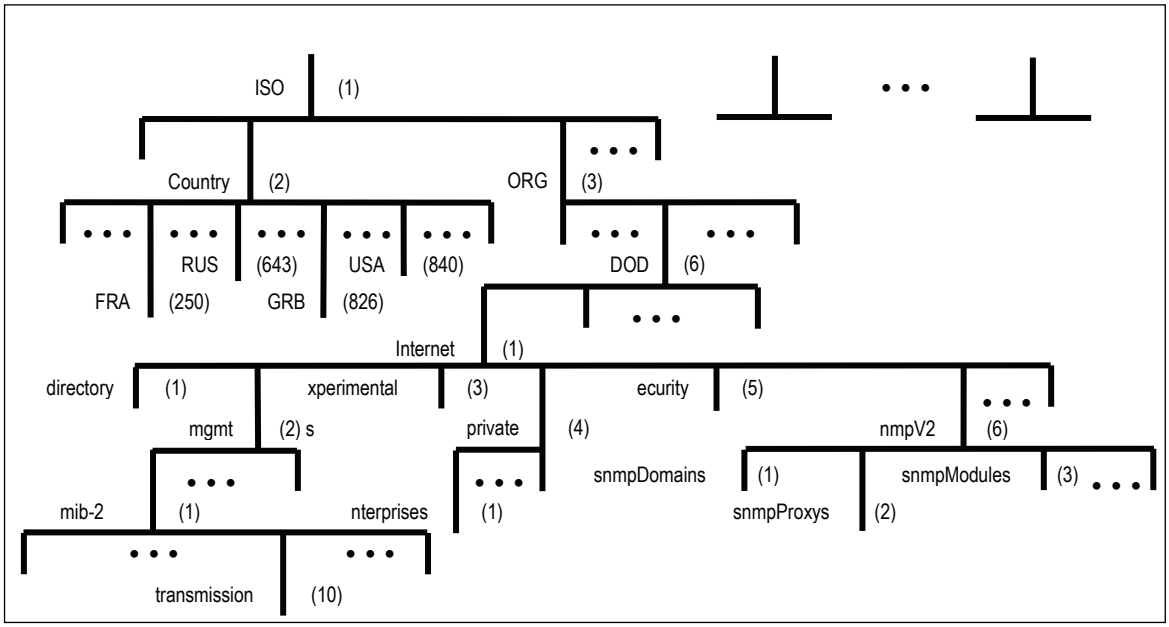


*Рис. 2. Корневое дерево иерархии данных для обеспечения сетевого управления, включая объектные идентификаторы стран*

**Предпосылка третья**. В Интернет-сети был разработан простой протокол обеспечения данными сетевого управления (Simple Network Management Protocol — SNMPv3), который в дальнейшем был усовершенствован, и в настоящее время стандартизирована третья версия этого протокола.

SNMPv3-стандарт представляет модульную структуру и, в частности, включает:

1. описание управляющей информации (База управляющей информации, Management Information Base — MIB и MIB2);

2. описание протокола.

В рамках SNMPv3-архитектуры используется вторая версия структуры информации для сетевого управления (Structure of Management Information — SMIv2). Данные для сетевого управления имеют иерархическую структуру, определяемую SMIv2, и рассматриваются как совокупность объектов сетевого управления, имеющих собственные уникальные идентификаторы (последовательности цифровых маркеров, разделённых точками, *object identifier*), и размещаемых в виртуальном MIB(2)-хранилище.

Высшим уровнем иерархии (рис. 2) для данных сетевого управления является Международная организация по стандартизации, имеющая кодировку «1» («iso» = 1). В частности, кодирование корневого дерева иерархии данных сетевого управления (*the path to the root*) имеет следующий вид:

```
org         OBJECT IDENTIFIER ::= { iso 3 }  --  «iso» = 1
dod         OBJECT IDENTIFIER ::= { org 6 }
internet    OBJECT IDENTIFIER ::= { dod 1 }
directory   OBJECT IDENTIFIER ::= { internet 1 }
mgmt        OBJECT IDENTIFIER ::= { internet 2 }
mib-2       OBJECT IDENTIFIER ::= { mgmt 1 }
security    OBJECT IDENTIFIER ::= { internet 5 }.
```

Одной из ветвей корневого дерева иерархии данных общего назначения является ветвь объектных идентификаторов стран (рис. 2), которая имеет вид:

```
country     OBJECT IDENTIFIER ::= { iso 2 }  --  «iso» = 1
RUS         OBJECT IDENTIFIER ::= { country 643 }
```

USA OBJECT IDENTIFIER ::= { country 840 }
GRB OBJECT IDENTIFIER ::= { country 826 }
FRA OBJECT IDENTIFIER ::= { country 250 } .

Таким образом, каждое государство (страна), фактически имеет свой объектный идентификатор, кодируемый как последовательность цифровых маркеров: 1 (ISO). 2 (страны). 643 (Российская Федерация). ... . Другими словами любая трехмаркерная последовательность вида «1.2. ... .» определяет государственную принадлежность объекта управления, находящегося в MIB(2)-хранилище.

**Способ**

Исходя из предыдущего анализа, предлагается использовать объектные идентификаторы стран (например, 1.2.643, Россия) в качестве префикса глобальной маршрутизации в IPv6-адресах. Таким образом, весь диапазон IPv6-адресов будет разделён на три больших диапазона:

1. национальные поддиапазоны IPv6-адресов государств;

2. поддиапазоны специальных адресов, в которые, в том числе, входят локальные, групповые и все иные технологические IPv6-адреса;

3. не используемые IPv6-адреса (запрещённые к использованию).

Примером такого глобального деления могут служить коды стран, используемые в системах фиксированной и мобильной телефонной связи (например, «+7» — Россия).

В шестнадцатеричном коде Российский диапазон IPv6-адресов будет иметь вид: 1264:3000::/20 . Диапазон IPv6-адресов США: 1284::/20.

**Причины и следствия**

Причинами и следствиями реализации предлагаемого способа являются:

- глобализация Интернет-сети, которая привела к созданию практически во всех странах мира национальных информационных обществ (электронных правительств), превратившихся в новую социально-экономическую среду (СоцЭС) [5]. В каждой стране такая СоцЭС стала сферой экономических интересов, также требующей своей защиты, как от внешнего, так и от внутреннего вмешательства;
- предлагаемый способ фактически вводит виртуальные границы национальных информационных обществ и СоцЭС. По аналогии со странами Шенгенской зоны, виртуальные границы остаются открытыми и прозрачными. Однако между странами Шенгенской зоны остаются государственные и административные границы, которые определяют зоны экономической, финансовой, юридической, экологической и др. ответственности государств. Т.е. между ними остаётся «межа», которая разделяет сферы тех или иных интересов государств. Также, и виртуальные границы национальных информационных обществ, фактически, являются «межой» в мировом виртуальном пространстве. Таким образом, предлагаемый способ разграничивает сферы интересов государств в мировом виртуальном пространстве;
- по аналогии с национальными радиочастотными диапазонами, каждый национальный поддиапазон IPv6-адресов будет являться национальным достоянием конкретного государства. Эксплуатация такого поддиапазона может стать источником пополнения государственного бюджета. Например, индивидуальные IPv6-адреса могут выдаваться гражданам Российской Федерации на безвозмездной основе пожизненно. Коммерческие организации могут брать в аренду необходимые для них фрагменты (причём уникальные, не повторяющиеся и в различных объёмах) национального поддиапазона IPv6-адресов на возмездной основе. В настоящее время, операторы сотовой связи пополняют государственную казну, оплачивая аренду того или иного частотного поддиапазона;
- ведение базы данных национального поддиапазона IPv6-адресов и жёсткий учёт и контроль используемых и не используемых IPv6-адресов обеспечат точное выявление киберпреступника и

любого нарушителя, осуществляющего противоправную деятельность в российском сегменте мирового информационного общества. В частности, попытки потенциальных внутренних нарушителей использовать не используемые IPv6-адреса будут пресекаться путём блокирования соответствующих IPv6-пакетов самой национальной информационно-технологической инфраструктурой (ИТИ), составляющей основу информационного общества (электронного государства). Это утверждение базируется на неукоснительном выполнении «принципа неотвратимости наказания»;

- при попытках виртуального проникновения киберпреступников с применением неиспользуемых IPv6-адресов в российскую СоцЭС, их действия будут пресекаться на границе национального информационного общества, т.е. национальной ИТИ. А при использовании потенциальным нарушителем действующего IPv6-адреса, факт прохождения IPv6-пакета с таким адресом будет фиксироваться на виртуальной границе, и если нарушение ИБ произойдёт, то материалы расследования киберпреступления будут переданы той стране, чей IPv6-адрес использовался (т.е. входил в национальный поддиапазон IPv6-адресов этой страны);

- по аналогии с существующей практикой, организации, предоставляющие услуги доступа в Интернет-сеть (Интернет-провайдеры), будут брать в аренду уникальные (не перекрывающиеся) фрагменты национального поддиапазона IPv6-адресов за соответствующую плату. IPv6-адреса Интернет-провайдера будут предоставляться его клиентам на основании соответствующих договоров на постоянной или временной основе. Это позволит однозначно установить клиента Интернет-провайдера, совершившего то или иное противоправное действие в киберпространстве. Это касается и организаций, и частных лиц, создающих на основе услуг Интернет-провайдеров WWW-сайты, содержащие экстремистскую, порнографическую и т.п. информацию.

- для законопослушных граждан и сотрудников организаций, пользователей Интернет-сети, практически ничего не изменится. Как они предоставляли свои персональные данные при заключении договоров с Интернет-провайдером, так и будут делать это в дальнейшем при переходе на IPv6-адресацию. За исключением одного: у них появится право выбора, т.е. пользоваться своими индивидуальными IPv6-адресами или предоставляемыми Интернет-провайдерами;

- в зонах свободного доступа к Интернет-сети, предоставляемого частными (благотворительными) организациями (например, сеть ресторанов быстрого обслуживания «McDonald's»), в зависимости от политик обеспечения ИБ этих организаций, пользователи Интернет-сети смогут также пользоваться, либо своими индивидуальными IPv6-адресами, либо предоставляемыми частными организациями, полагая, что последние арендуют уникальные фрагменты национального поддиапазона IPv6-адресов.

### Реализационные аспекты

**Международный аспект**. Первым шагом для реализации предлагаемого способа является официальная передача управления IPv6-адресным пространством в одну из всемирно признанных международных организаций (например, Международный союз электросвязи, Международная организация по стандартизации и др.). Возможно, для этого понадобится решение ООН, или только властей США.

Вторым шагом должно быть принятие ряда международных актов и стандартов, определяющих стратегию и политику, принципы и правила использования IPv6-адресного пространства, а также официальное закрепление за каждым государством своего уникального поддиапазона IPv6-адресов.

Третьим шагом должен быть определён период организационной и технологической адаптации (временной интервал перехода) национальных информационных обществ к полномасштабному применению своих поддиапазонов IPv6-адресов.

Четвёртым шагом может быть создание структурного подразделения «киберполиции» в рамках, например, Интерпола (Международная организация уголовной полиции), которое бы занималось расследованием международных киберпреступления, обеспечивало взаимодействие киберполицейских служб различных государств, выявляло неправомочное использование запрещённых IPv6-адресов и т.п.

**Национальный аспект**. Создание или назначение в каждой стране федерального органа исполнительной власти, отвечающего за разработку и реализацию стратегии и политики, принципов и правил использования национального поддиапазона IPv6-адресного пространства. В частности, в Российской Федерации указанный орган должен быть подчинён непосредственно Президенту РФ или Председателю Правительства РФ (или его Первому заместителю) и входить в состав, либо Администрации Президента РФ, либо Аппарата Правительства РФ. При этом федеральном органе должна быть образована общественная комиссия, в которой бы участвовали представители всех заинтересованных ведомств и организаций, включая общественные. Одной из задач такой комиссии могло бы стать разрешение всех возникающих конфликтов, связанных с распределением и эксплуатацией национального поддиапазона IPv6-адресного пространства, и выработка по ним соответствующих решений и рекомендаций.

**Технологический аспект**. Создание и ведение базы данных национального поддиапазона IPv6-адресов (IPv6-БД), а также жёсткий учёт и контроль используемых и не используемых IPv6-адресов. Эксплуатация IPv6-БД должна предусматривать соответствующую систему комплексной защиты базы данных [5,6]. А порядок доступа к ресурсам IPv6-БД должен быть регламентирован соответствующими федеральными нормативными правовыми актами. Сама IPv6-БД, как информационно-технологическая система (ИТС), может быть создана на основе государственно-частного партнёрства.

**Инфраструктурный аспект**. ИТИ любого государства, являющаяся основой национального информационного общества, должна включать специализированные средства контроля вредоносного и криминального трафика «по принципу»: пропускать IPv6-пакеты только с разрешёнными IPv6-адресами, к которым будут относиться:

1. национальные поддиапазоны IPv6-адресов государств;

2. поддиапазон специальных адресов, в который, в том числе, входят локальные, групповые и все иные технологические IPv6-адреса.

Всем государственным и частным организациям целесообразно провести настройки своих сетевых программно-аппаратных комплексов, исключающие обработку IPv6-пакетов с запрещёнными IPv6-адресами.

Порядок и правила использования локальных IPv6-адресов организациями и ведомствами должны предусматривать персональное назначение IPv6-адресов, т.е. закрепление за каждым работников своего уникального локального IPv6-адреса. Более того в локальных IPv6-адресах должен содержаться идентификатор государства и организации/ведомства [6]. В противном случае, организации или ведомства должны использовать уникальные (неповторяющиеся) поддиапазоны глобальных IPv6-адресов. Распределение и использование локальных IPv6-адресов в странах будет входить в сферу деятельности федеральных органов исполнительной власти, отвечающих за эксплуатацию национального поддиапазона IPv6-адресного пространства.

Порядок и правила применения трансляторов сетевых IPv6-адресов должны затрагивать преобразования локальных адресов в глобальные и наоборот только в рамках корпоративных (ведомственных) ИТС [5].

**Заключение**

Рассмотренный способ использования IPv6-адресации в мировом информационном обществе позволит резко снизить уровень киберпреступности и защитить национальные ИТИ государств без каких-либо ограничений прав и свобод граждан на получение объективной и независимой информации.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Интернет-ресурс*. www.startupafisha.ru/news/itogi-issledovaniya-kiberprestupnost-v-rossii-i-mi/$ (дата обращения: 20.12.2013).
2. *IETF. RFC 4291. S. Deering*, «IP Version 6 Addressing Architecture», February 2006 (http://www.rfc-editor.org/search/).
3. *IETF. RFC 2460. R. Hinden*, «Internet Protocol, Version 6 (IPv6) Specification», December 1998 (http://www.rfc-editor.org/search/).
4. *ISO*. «Codes for the representation of names of countries and their subdivisions», ISO 3166.
5. *Мельников Д.А.* Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. — М.: IDO Press, Университетская книга, 2012.
6. *Мельников Д.А.* Информационная безопасность открытых систем: Учебник. — М.: ФЛИНТА, Наука, 2013.