IPv6-protocol the logical characteristic properties used to increase the security level of national information technology infrastructures

D.A. Melnikov[1], S.V. Dvoryankin[1], A.P. Durakovskiy[1] and V.S. Gorbatov[1]
[1]National Research Nuclear University "Moscow Engineering Physics Institute", Moscow, Russian Federation
(DAMelnikov||SVDvoryankin||APDurakovskiy||VSGorbatov)@mephi.ru

***Abstract* - This paper suggests a method of IPv6-protocol the logical characteristic use to increase the security level of the national information technology infrastructures (e-governments) and global information community.**

I. INTRODUCTION

A constant growth of cybercrime in the Internet is annually observed, in 2012 alone the cost of cybercrime [1] is estimated at $ 2 bln in Russia and $ 110 bln worldwide.

"The figures speak for themselves". Given that, to identify cybercriminals still remains a difficult task whose solution cannot be found in most cases. This paper develops the concepts [2,3] and offers a method to reduce the complexity of the issue on the basis of IPv6-protocol the logical characteristic (RFC 2460 and RFC 4291 [4,5]) and standard ISO 3166 [6]. When the principle of inevitable punishment for cybercrime is strictly implemented, then the problem of managing any state and the entire world community information security (IS) would be solved. However, the political will of the leading powers and adoption of relevant international acts and standards is the main requirement to achieve victory over cybercrime.

II. BACKGROUNDS

Statement 1. The shortage of version 4 IP addresses (IPv4) whose length is 32 bits is felt as most urgent in the Internet community. In the 90's the version 6 IP addressing (IPv6) system which defined the 128-bit length addresses was proposed [2,3]. The total capacity of the IPv6 addresses space is $2^{128} \approx 10^{39}$. Such number of IPv6 addresses is much greater than the Earth's population.

The standards [4,5] presented in Fig. 1 define the global unicast IPv6 addresses encoding format.

The global routing prefix is (typically hierarchically-structured) a value assigned to a site (a cluster of subnet/links), and the subnet identifier (ID) is an identifier of a link within the site.

All global unicast addresses have a 64-bit interface ID field (i.e., $n + m = 64$), formatted.

n bits	*m bits*	*128-n-m bits*
Global routing prefix	Subnet identifier	Interface identifier

Figure 1. The global unicast IPv6 addresses encoding format

DOI: 10.978.819252/12213

Statement 2. In 1974 International Organization for Standardization (ISO) adopted the first version of the International standard ISO 3166 [6] which defines the code names of States and dependent territories as well as the main administrative units within the States. In accordance with the International standard the three digits designation was bound to each country, for example, 643 to Russia, 840 to USA, 826 to Great Britain, 250 to France.

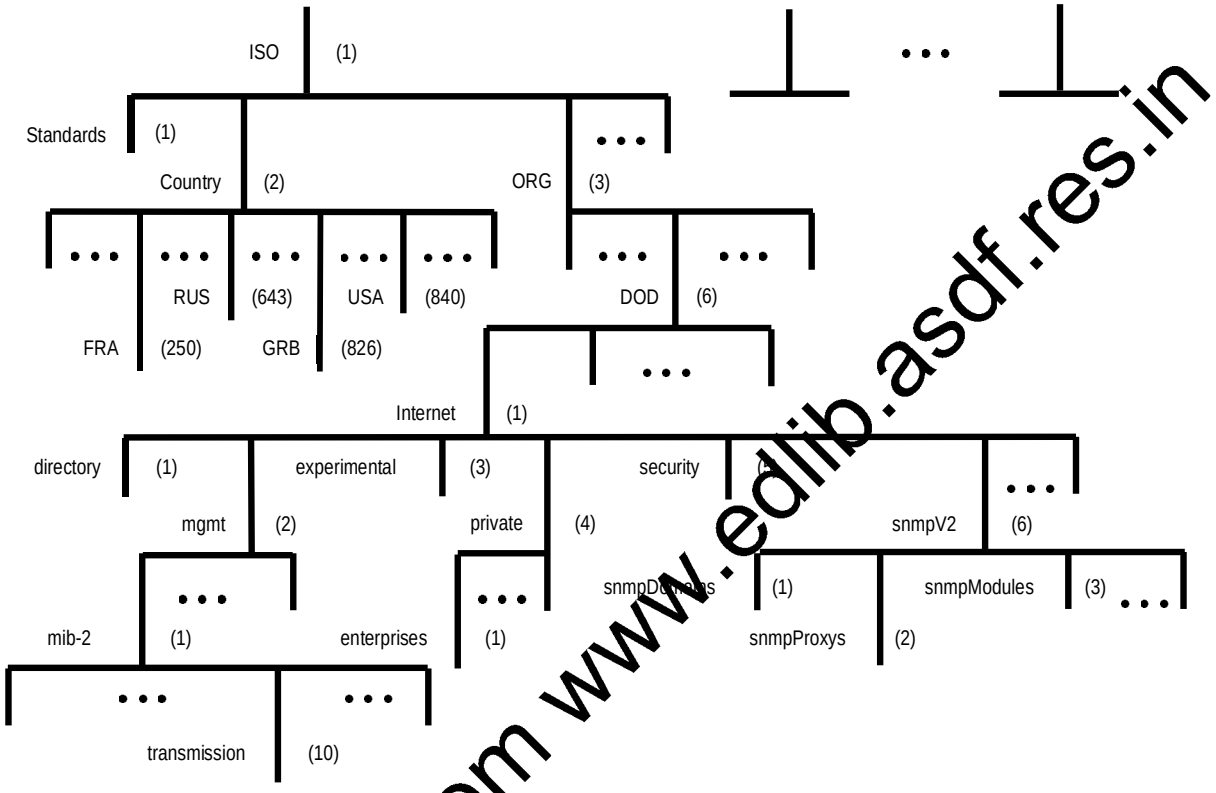

Figure 2. Root NMI hierarchy tree, including country object identifiers

Statement 3. In the Internet to develop a unified approach to the management of network hardware and software facilities Simple Network Management Protocol has been developed (SNMP). Later SNMP improved. Now a third version of SNMP (SNMPv3) is in practice.

SNMPv3 specifications are based on a modular architecture consisting of:

1) a data definition language;

2) definitions of management information (the Management Information Base, or MIB and MIB-II);

3) a protocol definition;

4) security and administration.

Within the SNMPv3 architecture Structure of Management Information second version (SMIv2) is applied. SMIv2 determines the hierarchy structure for the network management information (NMI) presented as a network management objects collection. Each object is bound to its own identifier (*object identifier* — OID). OIDs are sequences of digital labels separated by dots stored in MIB(-II).

For NMI ISO is in the highest hierarchy level (Fig. 2), "*iso*" = 1. In particular, coding of the path to the root (in NMI hierarchy tree) follows as:

DOI: 10.978.819252/12213

```
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 }
transmission OBJECT IDENTIFIER ::= { mib-2 10 }
experimental OBJECT IDENTIFIER ::= { internet 3 }
private      OBJECT IDENTIFIER ::= { internet 4 }
enterprises  OBJECT IDENTIFIER ::= { private 1 }
security     OBJECT IDENTIFIER ::= { internet 5 }
snmpV2       OBJECT IDENTIFIER ::= { internet 6 } .
```

The country OIDs form one brunch of the NMI hierarchy tree (one path to the root). Fig. 2 shows such a branch:

```
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 } .
```

Thus, every country is bound to its own OID coded as a digital label sequence, for example, 1 (ISO). 2 (countries). 643 (Russian Federation). ... ; 1 (ISO). 2 (countries). 840 (USA). ... ; 1 (ISO). 2 (countries). 826 (Great Britain). ... ; 1 (ISO). 2 (countries). 250 (France). ... . In other words, the state of management object discussed and stored in MIB(-II) (including control, use etc.), is specified by any three labels sequence of type “1.2. ... .”.

III. TECHNIQUES

Based on the above analysis, the paper offers to use countries OIDs (example, 1.2.643 — Russia) as the global routing prefixes in IPv6 addresses. Thus, it the IPv6 addresses space need be split in three big clusters of:

1) national IPv6 addresses subranges of countries;

2) special IPv6 addresses subrange, including local, multicast and any technological IPv6 addresses;

3) forbidden IPv6 addresses (an international organization should take a decision to use IPv6 addresses not included in the above first and second subranges). These IPv6 addresses must not be used until a decision to use them is made.

The countries’ codes used in the fixed and mobile telephony systems could be an example of such a global splitting up, i.e., each country is bound to its own international telephony code (identifier). Examples: “+7” to Russian Federation; “+1” to USA; “+44” to Great Britain; “+33” to France etc.

Hexadecimal coding of IPv6 addresses subranges for some countries might look as follows:

1) Russia — 1264:3000::/20.

2) USA — 1284:0::/20.

3) Great Britain — 1282:6000::/20.

4) France — 1225:0::/20 .

IV. MOTIVES AND EFFECTS

The motives behind the method offered and its effects may be the following.

DOI: 10.978.819252/12213

1) The Internet globalization which resulted in building national information communities (e-governments), practically in all the countries of the world. National e-governments will be transformed to new social economic environments (SEE) [7]. In each country, such an SEE becomes a sphere of special economic interests which requires protection, both from external and internal interventions.

2) The method offered actually delimits virtual national information communities and SEEs. By analogy with the Schengen countries, virtual borders remain open and transparent. However, there are the state and administrative borders between the countries of the Schengen zone. Such borders determine the zones of economic, financial, legal, environmental and other state responsibilities, meaning a boundary slip between them, which splits up the spheres of state interests. Similarly, the virtual borders of the national information communities actually become boundary slips in the worldwide virtual space. Thus, the offered method splits up the spheres of state interests in the worldwide virtual space.

3) By analogy with the national radio frequency bands, each national IPv6 addresses subrange will be public national property of a state and maintaining and servicing such subranges could be a source of the state budget replenishment. For example, Russians (or other country citizens) could get individual IPv6 addresses free throughout their life. Commercial organizations could rent the national IPv6 addresses subrange fragments (unique, not duplicate and in various amounts) on a paid basis. Now mobile and cellular communications providers replenish national incomes by payments of radio frequency band rent.

4) Maintaining national IPv6 addresses subrange data base (IPv6 NDB) and strict registration and control of used and unused IPv6 addresses will provide an exact identification of cyber criminals and any intruders who conduct illegal activities in Russian or other country domain of global information society. In particular, national information technology infrastructure (ITI), which is the basis of the information society (e-government), will pluck potential internal violators' attempts to use forbidden IPv6 addresses by a block of malicious IPv6 datagrams. The strict implementation of inevitable punishments is the base of the assertion above.

5) When cybercriminals make attempts of virtual penetration into Russian or other country' SEE by using forbidden IPv6 addresses, their actions will be intercepted at the boundary of the national information society, i.e. at the boundary of the national ITI. Moreover, when the potential violators use legitimate IPv6 address, the fact of passing IPv6 packet with this address will be recorded on the virtual border. If the information security violation does occur, the cybercrime investigation materials will be transferred to that country whose IPv6 address was used (i.e. from the national IPv6 addresses subrange of that country);

6) By analogy with the existing practice, the Internet service providers will rent unique (non-overlapping) parts of the national IPv6 addresses subrange for the appropriate payment. Internet service providers will assign IPv6 addresses to the clients on the basis of a particular permanent or temporary agreement.

This will uniquely identify that an Internet service provider's client performed a wrongful act in cyberspace. This can be also applied to organizations and individuals, creating Web sites of extremist, terrorist, pornographic and other malicious information on the base of the Internet-providers services.

7) For law-abiding citizens and organizations as Internet users, nothing will change impact. As they provide their personal data when signing agreements with Internet providers, they will go on doing so later during the transition to

DOI: 10.978.819252/12213

IPv6 addressing with only one exception: they will have the right to use their individual IPv6 addresses or provided by Internet providers.

8) The Internet users in the zones of free access to the Internet provided by private or charitable organizations (for example, a network of fast food restaurants "McDonald's") could also use their individual IPv6 addresses or provided by private organizations depending on their information security policies. In this case, it is expected that private or charitable organizations will use some unique non-overlapping parts of the national IPv6 addresses subrange.

V. IMPLEMENTATION ASPECTS

International aspect. First, for the implementation of the offered method, an official transfer of IPv6 address space authority must be established by a generally accepted international organization (e.g. International Telecommunication Union, International Organization for Standardization and other). To this end a decision of UN or only US authorities can be accepted.

Second, adoption of some international acts and standards will determine the strategy, policy, principles and rules of the IPv6 address space use as well as official selection of unique IPv6 addresses subranges for each country.

Third, a transient period for national ITIs should follow while adapting the worldwide system (the time transition interval) to a full-scale use of their IPv6 addresses subranges.

Fourth, an organization of "cyber police" within, for example, the Interpol (International Criminal Police Organization) can be established to investigate international cybercrime, provide national cyber police services interaction and detect unauthorized prohibited IPv6 addresses use.

National aspect. Each country should establish or assign a federal authority to create and implement national IPv6 addresses subrange use strategy, policy, principles and rules. In particular, in the Russian Federation such an authority can be subordinate directly to the President of the Russian Federation or to the Prime Minister of the Russian Federation (or his First Deputy) and be a part of the Administration of the President of the Russian Federation or the Executive Office of the Government of the Russian Federation. The federal authority shall form the Public Commission, in which representatives of all interested agencies and organizations, including the public ones will work. One of the objectives of such a Commission would be to resolve all the conflicts that related to the distribution and operation of the national IPv6-address space subrange, and to frame the necessary decisions and recommendations.

Technological aspect. IPv6-NDB must be created and maintained to control used for forbidden IPv6 addresses. The IPv6-NDB maintenance should include an appropriate DB complex protection system and a control access system operation should be regulated by federal legal acts.

IPv6-DB as information technology system (ITS) may be created on a state-private partnership base.

Infrastructural aspect. Any state ITI serving as a national information community base should include malicious and criminal traffic controls using the principle of skipping IPv6 packets with permitted IPv6 addresses only such as:

1) national IPv6 addresses subrange of states,

2) and special IPv6 addresses subrange, including local, multicast and any technological IPv6 addresses.

DOI: 10.978.819252/12213

In addition, all state and private organizations maintaining and developing national ITI should configure their software and hardware network devices (routers, switchers, etc.) in order to prohibit processing IPv6-packets with forbidden IPv6-addresses.

The procedures and rules of local IPv6 addresses use by organizations and agencies should provide a personal assignment of local IPv6 addresses, i.e. a unique local IPv6 address should be bound to its employee. Local IPv6 addresses must include state and organization/agency OIDs [8], otherwise, organizations and agencies must use their unique (non-overlapping) local IPv6 addresses subranges. Local IPv6-addresses distribution and maintenance in the countries will be part of the activities of the federal authority responsible for creating and implementing strategy, policy, principles and rules of national IPv6 addresses subrange use.

The procedures and rules of translators IPv6 addresses [7] use must include a conversion of local addresses to global ones and vice versa via corporate (agency-level) IT systems only.

VI. SUMMARY

A method and a system of IPv6 addresses use in the global information community can significantly reduce the cybercrime level and protect national ITI of states without any limitations of their rights and freedom of citizens to get true and independent information.

ACKNOWLEDGMENT

This work is performed in National Research Nuclear University "MEPhI" with the financial support of the Ministry of education and science of the Russian Federation in the framework of the project "Creation of the engineering and technical solutions for high-tech production of innovative software and hardware of information protection on the basis of perspective high-speed interfaces of information interconnection" jointly with JSC "OKB SAPR" in accordance with contract № 02.G25.31.0050.

REFERENCES

[1] Internet-resource. *http://www.startupanalyka.ru/news/itogi-issledovaniya-kiber-prestupnost-v-rossii-i-mi/$*.
[2] APNIC-089. "*IPv6 address allocation and assignment policy*". Version 012, 18 February 2013. Internet-resource. *http://www.apnic.net/policy/ipv6-address-policy*.
[3] ITU-T. "*A Study on the IPv6 Address Allocation and Distribution Methods*". 28 July 2009. Internet-resource. *http://www.itu.int/dms_pub/itu-t/oth/3B/02/ T3B020000020002PDFE.pdf*
[4] RFC 4291. Hinden, R. and S. Deering, "*IP Version 6 Addressing Architecture*», February 2006.
[5] RFC 2460. Deering, S. and R. Hinden, "*Internet Protocol, Version 6 (IPv6) Specification*", December 1998.
[6] International Organization for Standardization. "*Codes for the representation of names of countries and their subdivisions*", ISO 3166, 1974.
[7] Melnikov D.A., "*Organization and information security management of information technology networks and systems*": Textbook. — M.: IDO Press, Universitskaya kniga, 2012, ISBN 978-5-91304-246-0, 978-5-4243-0004-2, (rus).
[8] Melnikov D.A. "*Open systems information security*": Textbook. — M.: FLINTA, Nauka, 2013, ISBN 978-5-9765-1613-7, 978-5-02-037923-7, (rus).

DOI: 10.978.819252/12213