УДК 681.3

О.В. Кобзар[1]
М.О. Кобзар[2]
[1]*Науково-дослідний центр Збройних Сил України «Державний океанаріум» м. Одеса, Україна*
[2]*Військова академія (м. Одеса), Україна*

РИЗИКИ ТА ЗАГРОЗИ УКРАЇНСЬКОМУ СЕГМЕНТУ МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ НЕСТАБІЛЬНОЇ ВОЄННО-ПОЛІТИЧНОЇ ОБСТАНОВКИ

В цій роботі авторами розглядається одна з проблем глобальної загрози національній безпеці України в кібернетичному просторі, що обумовлюється системними помилками, які, на думку авторів, були закладені в архітектуру вітчизняного сегменту мережі Інтернет ще на етапі його створення, що в умовах зростання рівня кібернетичних загроз державним і військовим органам управління, є вкрай небезпечним явищем.

В статті акцентується увага на актуальних питаннях забезпечення національної безпеки держави у кібернетичному просторі. В основу аналізу покладено діючу будову сегменту української мережі Інтернет.

Ключові слова: *інформаційно-телекомунікаційна мережа, Інтернет, кібернетичний простір, магістральна лінія зв'язку, мережа, вузол, сегмент, трафік*

Постановка проблеми

В умовах надзвичайно надскладної воєнно-політичної обстановки, яка останні роки супроводжує Україну, завдання забезпечення інформаційної безпеки держави має виняткову та першочергову актуальність.

Широке застосування комп'ютерних систем управління, обробки, збереження та передачі інформації у всіх сферах життєдіяльності України, в тому числі і у військовій сфері, змушує ще раз проаналізувати та мінімізувати ризики і загрози, виникнення яких може призвести до повного припинення інформаційної комунікації країни.

Практика експлуатації і розширення таких систем проводиться за принципом послідовного приєднання комп'ютерів до мережі. Разом з цим, звідкіля та яким чином виділяється та перенаправляється міжнародний трафік для України, знає та розуміє тільки вузьке коло фахівців.

Тому будь-які зміни або вторгнення в наявну систему міжнародного трафіку можуть викликати досить негативні і небажані наслідки. Так, наприклад, за повідомленням низки інформаційних агентств, група компаній російського інтернет-холдингу *Mail.ru* оголосила про припинення з 20.12.2016 доставки трафіку в точки обміну з Україною з причини того, що холдингу стало дорого поставляти в Україну свій трафік, але при цьому не виключаються і політичні причини. Подібна відмова може відобразитись, переважно, тільки на звичайних українських користувачах у вигляді зменшення швидкості доступу до сайтів і сервісів холдингу *Mail.ru*, низки популярних соціальних мереж, служб миттєвого обміну повідомленнями *ICQ* і *Агент*, служби електронної пошти *Mail.ru*, а також інших російських ресурсів або порталів *Mail.ru* та *My.com* [1].

Якщо подібні відкриті та контрольовані дії великих російських інтернет-холдингів створюють проблеми, в основному, тільки для мешканців України в побутовому сегменті інтернет-послуг, то повне припинення передачі трафіку з цього напрямку, в результаті фізичного навмисного вимкнення або, пошкодження наявних магістральних ліній зв'язку в Україну на напрямках Москва–Київ або (та) Москва–Львів, буде мати досить непередбачувані наслідки для всієї інфраструктури України, перш за все, у доступі до ресурсів, які розміщені за кордоном.

Так, наприклад, якщо на перший погляд, сервіси Державного банку «Ощадбанк» мають українську національність домену (ім'я домену – www.oschadbank.ua), то при детальному з'ясуванні, вони розміщені на серверах США (IP-адреса: 52.11.14.125), те ж можливо зазначити і стосовно сервісів українського «ПриватБанку» (ім'я домену – www.privatbank.ua), але вони також розміщені за кордоном, а саме на серверах Ірландії (IP-адреса: 54.76.248.123).

Аварійні ситуації мережі Інтернет різноманітного походження, навіть на локальному рівні та в зменшеному вигляді, можуть призвести до припинення доступу до мережі, як це сталося 26.11.2016 року в м. Одесі, коли в результаті пошкодження волоконно-оптичної магістральної лінії зв'язку, інтернет-зв'язок та інші види зв'язку були повністю відсутні в декількох районах міста та у користувачів низки місцевих провайдерів [2].

Аналіз останніх досягнень і публікацій

Аналіз досліджень, досягнень і публікацій із зазначеної тематики свідчить про те, що питанню підвищення живучості та резервування українського сегменту Інтернету приділяється не досить значна увага та немає прямої акцентуації проблеми. Доказом цього є той факт, що дослідники, в основному, вивчають внутрішні проблеми та загрози вже сформованої системи вітчизняного сегмента Інтернету, а зовнішні ризики залишаються поза їх увагою.

Вихідні дані для аналізу були отримані з доступних відкритих джерел інформації.

З числа вітчизняних публікацій останнього часу на увагу заслуговує дослідження основних параметрів українського сегменту Інтернету як складної мережі, що були опубліковані у випуску № 40 Збірника «Відкриті інформаційні та комп'ютерні технології» [3].

Цікавими висновками зазначеної публікації стали насамперед:

по перше, той факт, що 907 автономних систем українських вузлів анонсуються в точку обміну або одним шляхом (AS-path), або реекспортом через єдиного їх сусіда та з математичної точки зору, вони є вершинами графа зі ступенем 1;

по друге, більшість українських вузлів українського сегмента Інтернету не є транзитними і стануть ізольованими від точки обміну при розриві їх єдиного зв'язку;

і головне, українські вузли здатні обмінюватися трафіком з іншими українськими вузлами через вузли, які перебувають поза українським сегментом Інтернету.

Також як досить відчутне досягнення можливо роглядати повідомлення від 30.11.2016, в якому заступник міністра оборони України Олександр Дублян оприлюднив інформацію щодо початку створення в Україні Центру оперативного реагування на кіберзагрози, матеріально-технічну базу якого забезпечують США. Цей захід був також передбачений в плані реформування Міноборони України [4].

Реалізація цих та інших результатів наукових, науково-дослідних та організаційно-технічних заходів дозволить нейтралізувати частину ризиків та загроз українському сегменту мережі Інтернет.

Постановка задачі та її розв'язання

З огляду на зазначені проблеми, метою цієї роботи є аналіз чинної системи українського сегмента Інтернету як складної мережі та пропозиції щодо основних шляхів її удосконалення, підвищення живучості та резервування.

Виділення невирішених раніше частин загальної проблеми, яким присвячується стаття

Врахування факторів ризиків та загроз українському сегменту мережі Інтернет, надання пропозицій щодо створення і розгортання додаткових основних (резервних) хабів (точок обміну трафіком) з прямим виходом на європейські та азійські вузли обміну. Особливу увагу при цьому необхідно зосередити на створенні двох-трьох нових швидкісних волоконно-оптичних магістралей на західному напрямку, а на південному – потужної підводної волоконно-оптичної магістральної лінії зв'язку по дну Чорного моря.

Виклад основного матеріалу досліджень з повним обґрунтуванням отриманих наукових результатів

В рамках цієї наукової статті розглянуті основні підходи до оцінки параметрів українського сегмента Інтернету як складної мережі та в дещо ширшому ракурсі, аніж того, що ще досить недавно вбачили

фахівці, які досліджують архітектуру побудови Інтернету. Цілком зрозуміло, що на той час не існувало тих загроз, з якими наша країна зіткнулася в останні два роки, тому вони майже не розглядалися.

Як відомо, на фізичному рівні Інтернет представляє собою мережу хабів (точок обміну трафіком), пов'язаних між собою магістральними каналами (рис. 1). У точках обміну трафіком концентрується не тільки трафік, але і мережева інфраструктура (дата-центри, хостинг тощо) та здійснюється передача пакетів даних між різноманітними частинами мережі, в нашому випадку (Україна) – між територією конкретного регіону і міжнародним Інтернетом.

Найбільші точки обміну розташовані у містах: Нью-Йорку, Лондоні, Франкфурті, Парижі та Амстердамі, які входять в п'ятірку основних хабів.

У списку найбільших точок обміну трафіком в світі лідирують DE-CIX (пікова пропускна здатність – 5178 Гбіт/с), AMS-IX (4270 Гбіт/с). Російська точка обміну трафіком MSK-IX перебуває на п'ятому місці (2135 Гбіт/с). Сукупна пропускна всіх міжнародних каналів зв'язку на 2015 рік становила 180 Тбіт/с.

За кількістю міжнародних каналів Європа тривалий час була абсолютним лідером, перевершуючи будь-який інший континент, але зараз їх приблизно стільки ж, як і у Північній Америці (за рахунок США). Азія, Південна Америка та Африка займають наступні позиції, але Європа всеодно залишається ключовим вузлом у глобальній мережі [5].

Європейський вузол відрізняється від інших континентів ще однією деталлю: близько 70 % міжнародного трафіку переміщається між містами всередині континенту. Для порівняння, у Південної Америки і Африки прямо протилежна картина: 80 % каналів йдуть до інших континентів, 60 % зовнішніх каналів Південної Америки підключені до одного зарубіжного міста Маямі (США). Таким чином, якщо в Маямі трапиться блекаут, з інтернету частково випаде майже вся Південна Америка.

Рис. 1. Розподіл потужності обміну трафіком поміж континентами

Подібна ситуація, але безперечно в менших масштабах, може очікувати і Україну, яка в свій час масово була під'єднана до ресурсів російських хабів, що обумовлювалося наявністю на той час досить розвиненої мережі наземних комунікацій зв'язку, яка залишилася ще з часів єдиного інформаційного простору країн колишнього СРСР та яка була модернізована в більш пізніший період.

На візуалізованій схемі Європейського сегмента Інтернету показано мережу хабів (точок обміну трафіком) та магістральних ліній, які проходять територією України та з'єднують напрямки Москва (17) – Київ (28), Москва (17) – Львів (окрема магістраль), а також дві транзитні магістралі Москва (17) – Франкфурт (2) та Москва (17) – Амстердам (4) (рис.2) [5].

З метою дослідження та оцінки параметрів українського сегмента Інтернету, групою авторів [3], було отримано анонси близько 3000 блоків IP-адрес (підмереж), отриманих від 1034 автономних систем.

На рис. 3 подано схему зв'язків автономних систем. Під вузлами (Autonomous System, AS) розуміється група IP-мереж, які належать одному або декільком операторам, та які мають одну, чітко визначену політику маршрутизації. Графічне зображення (вузли AS – точки, розміщені на дузі кола, зв'язки – хорди) дає уявлення про наявність явно лідируючих AS-вузлів, ступінь яких максимальний. Цими вузлами виявилися, перш за все, інтернет-гіганти DATAGROUP та UA-IX (139 та 88 зв'язків, відповідно), яким належить не тільки обладнання хабів, а й кабельні магістралі.

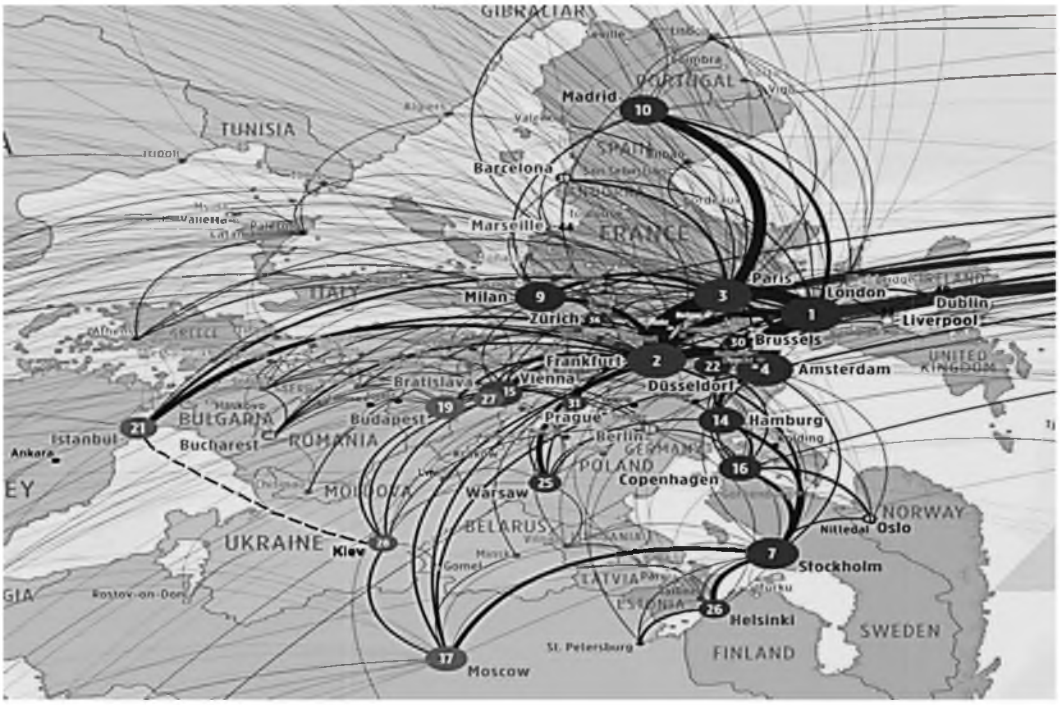

Рис. 2. Візуалізована схема Європейського сегмента мережі Інтернет
(нова окрема, частково підводна, волоконно-оптична магістраль, яка пропонується, для з'єднання хабів напрямку Київ (28) – Стамбул (21), зображена пунктиром)

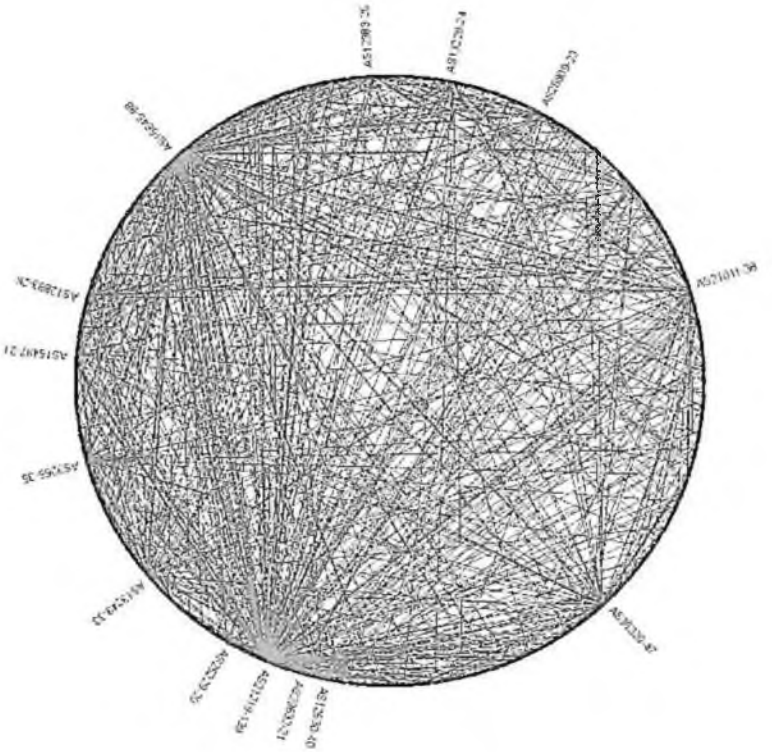

Рис. 3. Схема зв'язків українського сегмента Інтернет
(на схемі показані найбільші вузли та їх ступінь)

Для вивчення властивостей, пов'язаних з надійністю, захистом від вразливостей цієї мережі, авторами [3] була реалізована процедура виділення опорної мережі. В результаті була отримана опорна мережа українського сегмента Інтернету, що складається зі 128 основних вузлів, кожен з яких має ступінь, не менший, ніж 2 (рис. 4).

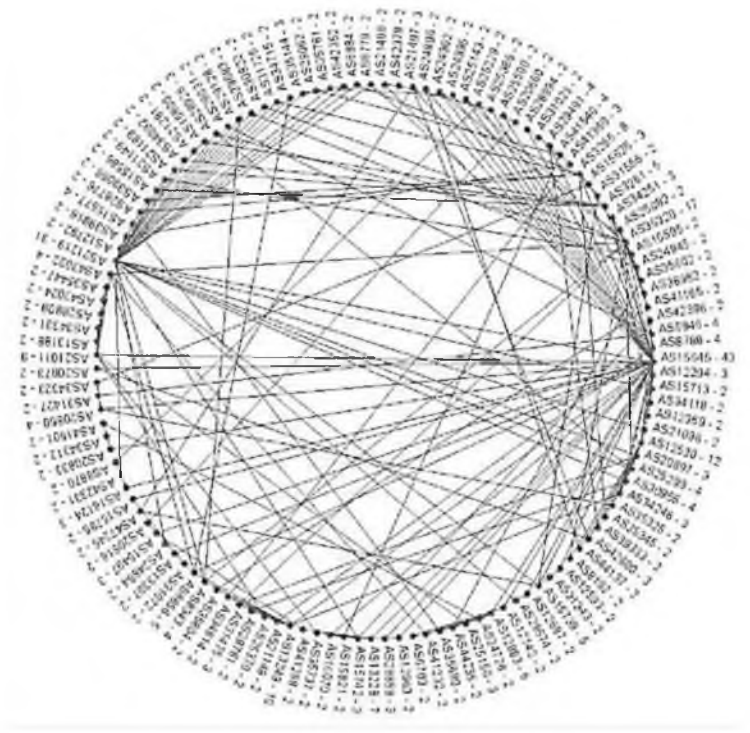

Рис. 4. Опорна мережа українського сегмента Інтернет, яка складається з вузлів зі ступенем 2 і вище

У п'ятірку вузлів опорної мережі з найвищим ступенем увійшли:

AS 15645 (UA-IX) – 43 зв'язки з вузлами, що мають ступінь 2 і вище;

AS 21219 (DATAGROUP) – 31 зв'язок;

AS 35320 (ETT) – 17 зв'язків;

AS 12530 (Golden Telecom) – 12 зв'язків;

AS 13249 (IT Systems) – 10 зв'язків.

DATAGROUP – провідний телекомунікаційний оператор на українському ринку комплексних послуг фіксованого зв'язку, який займає лідируючі позиції в основних сегментах: передача даних, міжнародний транзит трафіку, супутниковий зв'язок [6].

UA-IX – Українська мережа обміну трафіком, яка побудована на базі обладнання Extreme Networks і Cisco Systems, складається з декількох комутаторів, об'єднаних каналами зв'язку 40G Ethernet, і двох маршрутизаторів Cisco ASR 1001 [7].

Окрім наведених двох провідних операторів, в Україні діє ще низка менш потужних хабів (точок обміну трафіком), наприклад, таких як:

Ukrtel-IX – точка обміну трафіком ВАТ «Укртелеком», до якої під'єднані всі державні компанії та інші великі провайдери (вузли доступу до неї існують у всіх обласних і в більш ніж 100 районних центрах України);

X.UA – пірінгова точка обміну трафіком, що включає в себе мережу доставки і обміну медіа-трафіком, приватний VLAN в одній з точок обміну трафіком (Giganet, Dtel, UA-IX), IP-транзит, FTTB, FTTH;

OD-IX, M-IX, KH-IX, LV-IX, CH-IX – регіональні точки обміну трафіком м. Одеса, м. Дніпропетровськ, м. Харків, м. Львів, м. Чернігів (відповідно) та деякі інші.

Отже, фактично, вузли даної опорної мережі з максимальною кількістю вихідних ребер (ступенем) переважно мають високий рівень посередництва (низьким рівнем кластерного), що не дозволяє розглядати їх як основи для побудови кластерів при автоматичному групуванні, а скоріше як елементи, що з'єднують окремі групи вузлів. Відомо, що мережі з поважним розподілом ступенів вузлів називають безмасштабними (scale-free).

Також в результаті дослідження, можливо впевнено стверджувати, що з метою досягнення симетрії трафіку в мережі та забезпечення живучості і гнучкості українського сегмента Інтернету, необхідне з'єднання новими окремими додатковими швидкісними магістралями напрямку Київ (28) – Варшава (25) та Львів – Варшава (25), а також прокладення по дну Чорного моря нової окремої, частково підводної, волоконно-оптичної магістральної лінії для подальшого з'єднання хабів напрямку Київ (28) – Стамбул (21) (рис. 2).

Окремим варіантом, в доповнення до підводної волоконно-оптичної магістралі ITUR напрямком Одеса (Україна) – Стамбул (Туреччина) – Палермо (Італія), з метою підсилення системи, можливо розглянути технічну можливість щодо під'єднання України до підводного магістрального кабелю Caucasus Cable System, який перетинає Чорне море із заходу на схід від Болгарії до Грузії [8].

Рис. 5. Карта підводних кабелів мережі Інтернет
(*станом на 5 грудня 2016 р.)* (нова окрема, частково підводна, волоконно-оптична магістраль, яка пропонується для з'єднання вузла Київ (28) – підводна магістраль Caucasus, зображена пунктиром)

Висновки

Виходячи з вищезазначених характеристик та особливостей побудови українського сегмента Інтернету, можливо зробити висновок, що в умовах надзвичайно надскладної воєнно-політичної обстановки з метою підвищення його живучості та резервування Україна повинна вже в найближчий час розпочати створення двох-трьох потужних Дата-центрів, нових хабів (точок обміну трафіком) та розгалуженої мережі швидкісних волоконно-оптичних магістралей. При цьому, Україна повинна гарантовано оминути територію та, за можливості, поступово зменшувати трафік в точках обміну з країною, що здійснює агресію проти України.

Перспективи подальших досліджень

Напрямком подальших досліджень може стати визначення технічних особливостей щодо створення в Україні потужних хабів (точок обміну трафіком) світового рівня з прямим виходом на європейські та азійські вузли обміну, які будуть здатними забезпечити не тільки потреби України, а й бути транзитними (резервними) потужностями для країн близького та далекого зарубіжжя.

Список використаних джерел

1. *Російський інтернет-гігант Mail.ru припиняє доставляти трафік в точки обміну трафіком в Україні [Електронний ресурс]. – Режим доступу : https://politeka.net/369008-rossiyskiy-internet-gigant-otkazalsya-postavlyat-trafik-v-ukrainu.*

2. *Аварія на лінії [Електронний ресурс]. – Режим доступу : http://icn.ua/posts/avariya-na-linii.*

3. *Фурашев В.Н., Зубок В.Ю., Ландэ Д.В.. Параметры украинского сегмента Интернет как сложной сети / В.Н. Фурашев, В.Ю. Зубок, Д.В. Ландэ // Открытые информационные и компьютерные технологии. – 2008. – Выпуск 40. – С. 235–242.*

4. *В Україні за підтримки США розпочали створення Центру реагування на кіберзагрози. [Електронний ресурс]. – Режим доступу : http://tyzhden.ua/News/179736.*

5. *Кровоносна система світового Інтернету [Електронний ресурс]. – Режим доступу :https://habrahabr.ru/company/rootwelt/blog/305634.*

6. *DATAGROUP – провідний телекомунікаційний оператор на українському ринку комплексних послуг фіксованого зв'язку [Електронний ресурс]. – Режим доступу : http://www.datagroup.ua/uk.*

7. *Технічний опис Української мережі обміну трафіком UA-IX [Електронний ресурс]. – Режим доступу : http://www.ix.net.ua/ru/o-kompanii/tehnicheskoe-opisanie.*

8. *Карта підводних кабелів світової мережі Інтернет (станом на 5 грудня 2016) [Електронний ресурс]. – Режим доступу : http://submarine-cable-map-2016.telegeography.com.*

Рецензент: Г.П. Фердман, к.держ.упр., с.н.с., Науково-дослідний центр Збройних Сил України «Державний океанаріум», м. Одеса, Україна

РИСКИ И УГРОЗЫ УКРАИНСКОМУ СЕГМЕНТУ СЕТИ ИНТЕРНЕТ В УСЛОВИЯХ НЕСТАБИЛЬНОЙ ВОЕННО-ПОЛИТИЧЕСКОЙ ОБСТАНОВКИ

А.В. Кобзарь, М.А. Кобзарь

В данной работе авторами рассматривается одна из проблем глобальной угрозы национальной безопасности Украины в кибернетическом пространстве, обусловленных системными ошибками, которые, по мнению авторов, были заложены в архитектуру отечественного сегмента сети Интернет еще на этапе его создания, что в условиях роста уровня кибернетических угроз государственным и военным органам управления, является крайне опасным явлением. В основу анализа положено действующее строение сегмента украинской сети Интернет.

Ключевые слова: *информационно-телекоммуникационная сеть, Интернет, кибернетическое пространство, магистральная линия связи, сеть, узел, сегмент, трафик*

RISKS AND THREATS TO UKRAINIAN SEGMENT OF THE INTERNET IN AN UNSTABLE MILITARY AND POLITICAL SITUATION

A. Kobzar, M. Kobzar

The authors considered one of the problems of global threats to national security of Ukraine in cyberspace. They are depending on the system errors that, according to the authors, were laid in the architecture of the domestic segment of the Internet is still at the stage of its creation. in a growing level of cyber threats to state and military authorities, this is a very dangerous phenomenon. The basis of the analysis put the current Ukrainian Internet segment.

Keywords: *information and telecommunications network, Internet, cyberspace, communication backbone, network, host, segment, traffic.*

Надійшла до редакції 02.12.2016