СУЧАСНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА УКРАЇНИ І ОСНОВНІ ЗАВДАННЯ ЩОДО ЇЇ ЗАХИСТУ

О.Д. Довгань
головний науковий співробітник
Науково-дослідного інституту інформатики і права
Національної академії правових наук України,
кандидат юридичних наук,
старший науковий співробітник

Постановка проблеми. Процеси глобалізації, каталізатором яких в останні десятиріччя стала інформатизація на основі електронних технологій, крім свого позитивного значення для розвитку прогресу зумовлюють появу нових викликів і загроз для інформаційної інфраструктури, національного інформаційного суверенітету, самобутності, самосвідомості, а для цивілізації – багатоваріантних можливостей подальшого розвитку. І тому робота з нейтралізації загроз як важливої складової забезпечення інформаційної безпеки є запорукою ефективного використання і перспективного розвитку суверенних для кожної держави, нації масивів інформації. Розвиток ефективних інструментів забезпечення інформаційного суверенітету є важливою умовою суспільного розвитку і першочерговим завданням сьогодення. Зазначене обумовлює актуальність обраної теми дослідження.

Аналіз останніх досліджень та публікацій. Проблеми глобалізації, їх вплив на інформаційну безпеку знаходять своє відображення в науковій літературі, зокрема в роботах Д.Белла, М.Кастельса, І.Валлерстайна, С.Хоффмана та ін., питання національного інформаційного розвитку – у роботах В.Горового, О.Онищенка, В.Пилипчука, В.Попика та ін. Разом із цим, у зв'язку із загостренням проблеми своєчасного правового забезпечення сучасних динамічних інформаційних процесів, зростання числа загроз, актуалізується потреба аналізу сучасної інформаційної інфраструктури та основних завдань щодо її захисту.

Метою статті є визначення особливостей сучасної інформаційної інфраструктури та основних завдань щодо її захисту.

Основні результати дослідження. Поняття інформаційної інфраструктури визначається як сукупність програмно-технічних засобів, інформаційних комунікацій, інших механізмів управління інформаційними ресурсами, напрацьованих суспільною практикою, організаційних систем збереження і використання наявних обсягів інформації, а також інститутів продукування

нової інформації в інтересах суспільного розвитку, засобів нормативного забезпечення інформаційної діяльності, захисту вітчизняних інформаційних ресурсів від усіх видів загроз та негативних впливів. Призначення цієї інфраструктури полягає в забезпеченні суспільства необхідними для його існування і розвитку інформаційними ресурсами.

Суверенні інформаційні масиви у структурі цих ресурсів мають з огляду на об'єктивні потреби розвитку вітчизняного суспільства в умовах глобалізації основоположне значення. Вони є в умовах сучасної глобалізації заснованим на національній традиції орієнтиром для суспільного розвитку, еволюції самої інформаційної основи, подальшого інформаційного виробництва, дороговказом у механізмах інформаційних обмінів у системі внутрішньо українських інформаційних комунікацій та в міжнародному інформаційному співробітництві. Від ефективного використання вітчизняної інформаційної інфраструктури значною мірою залежить забезпечення і розвиток національного суверенітету, що в умовах сучасних глобальних перетворень є основним показником зберігання національної самобутності, важливою умовою підтримки міжнародних відносин на партнерському рівні. Її розвиток та інтеграція належить до основних стратегічних цілей формування інформаційного суспільства в Україні [1]. Забезпечення її функціонування і розвитку визначається потребами зберігання змісту суспільно значущих масивів інформації.

Як свідчить досвід передових в інформаційному розвитку країн світу «ефективна інформаційно-комунікаційна інфраструктура (ІКІ) – визначальна складова стратегії забезпечення національного інформаційного суверенітету, яка дає можливість державі поширювати свої суверенні права на певний сегмент глобального інформаційного простору. Водночас ІКІ – це показник економічного потенціалу країни. А цей потенціал, у свою чергу, є матеріально-технологічною базою, на основі якої здійснюється інтегрованість у глобальний інформаційний простір і яка також стає дедалі важливішим чинником визначення тієї ролі, яку вона відіграє у світовому розподілі праці» [2].

Ставка на розвиток інформаційно-комунікаційної структури в поєднанні з іншими інноваційними проектами забезпечує цим країнам прорив у сфері високих технологій, сприяє успішній роботі найефективнішої і базової для всіх інших напрямів розвитку галузі економіки – виробництва інформації, нових знань. Осмислене здійснення цих изначальних структурних перетворень в економіці забезпечило провідну роль даних країн у світовій економіці.

Так, державна програма Південної Кореї у сфері інформаційних технологій «Базова національна інформаційна система» (National Basic Information System), що була розроблена на початку 1980-х років і почала виконуватися в 1987 р., поєднала загальну комп'ютеризацію та розвиток інформаційних технологій з економічним зростанням країни. На початку 1990-х років програма була переглянута і у квітні 1994 р. прийнято проект «Національна інформаційна супермагістраль» (National Information SuperHighway), що дістав у 1995 р. назву «Корейська інформаційна інфраструктура» (Korea Information Infrastructure). Здійснення цього довгострокового плану за задумом уряду –

це ключова ланка в переході Південної Кореї від індустріальної економіки, що розвивається, до економіки розвинутої держави [3].

У США в 1993 р. Робочою групою з інформаційної інфраструктури (Information Infrastructure Task Force) було запропоновано дев'ять базових принципів державного регулювання: заохочення приватних інвестицій; концепція універсального доступу; допомога в технологічних інноваціях; забезпечення інтерактивного доступу; захист особистого життя, безпеки й надійності мереж; поліпшене управління спектром радіочастот; захист прав інтелектуальної власності; координаія державних зусиль; забезпечення доступу до державної інформації [4].

Важливим аспектом успішного використання національної інформаційної інфраструктури в США став розподіл і налагодження взаємодії функцій між державою та приватним сектором. Так, приватний сектор як головне джерело капіталу й експертів, має у відповідь на запити ринку визначити, які технології розвивати, установити стандарти, розвивати нові послуги й продукти. Держава ж, зі свого боку, може полегшити протікання цих процесів шляхом прийняття відповідних законів і адміністративного регулювання та за допомогою підтримки випробувань нових технологій. При цьому процес встановлення єдиних стандартів має бути відкритим і відбуватися за участю великих груп зацікавлених виробників.

Скоординовані дії держави, приватного сектору і громадських організацій є також характерною особливістю відповідного канадського досвіду [5]. При цьому показовий той факт, що країни, які мають найрозвиненішу інформаційну інфраструктуру, високий рівень розвитку інформаційних технологій, входять і до переліку країн з найвищим індексом конкурентоспроможності [6].

Відзначається зростаюча залежність суспільних інститутів від цих мереж і ця обставина стає додатковим стимулом для хакерських вправ. Із іншого боку, розвиток техніко-технологічної бази інформатизації, розширення доступу до виробництва і використання інформаційних ресурсів необмеженими масами користувачів створює зростаючі можливості не лише для впровадження електронного самоврядування, волевиявлення законослухняних громадян. Розвиток інформатизації дає змогу для прояву антисоціальних елементів, їх організацій. І, нарешті, в умовах становлення інформаційного суспільства, впливи на національну інформаційну структуру можуть також мати неправовий, диверсійний характер, стають метою інформаційних воєн. Тобто, кібертероризм впливає і, очевидно, надалі впливатиме, навіть у більшій мірі, виходячи із зростаючого рівня інформатизації, як на стан соціального здоров'я на рівні українського суспільства, так і в загальноцивілізаційних масштабах.

Слід зазначити, що до сьогодні розвиток технологій негативного впливу на інформаційну інфраструктуру відбувається швидше, ніж відповідних засобів протидії. Це пояснюється не лише засекречуванням подібних розробок у найбільш просунутих у комп'ютеризації країнах, використанням їх насамперед в оборонних інтересах. Значною мірою розробка засобів протидії кіберзагрозам у більшості держав із рівнем комп'ютеризації, еквівалентним українському, відбувається пасивно. Це пояснюється, насамперед, недостатнім усві-

домленням наявних небезпек на рівні прийняття загальносуспільних рішень, що, у свою чергу, пояснюється недостатньою комп'ютерною грамотністю, недостатнім усвідомленням ролі комп'ютеризації у сучасному суспільстві.

Зростаюче значення інформаційної інфраструктури в розвитку суспільного життя обумовлює відповідне підвищення значення організації інформаційної безпеки. Дане питання особливо важливе для України в сучасний період.

На сьогодні у розпорядженні України знаходиться сукупність різноманітних компонентів інформаційної інфраструктури: соціальні інформаційні комунікації, наявні інформаційно-аналітичні, бібліотечні, архівні та інші центри збереження й організації використання інформаційних ресурсів, наукові установи, структури, пов'язані із аналізом первинних масивів інформації типу «фабрика думки», дослідницькі фонди, соціологічні центри – всі структури, що займаються виробництвом суспільно значущої інформації, включаючи управлінську, економічну, політичну та для забезпечення всіх видів іншої суспільної діяльності, системи правотворчого регламентування інформаційної сфери. Ці компоненти інфраструктури є комп'ютеризованими і пов'язаними комп'ютерними мережами з усіма галузями господарчої діяльності, життєво важливими центрами суспільного життя. Тому саме ці компоненти вітчизняної інформаційної інфраструктури найбільш вразливі для кібернетичних загроз.

При цьому недостатня організація захисту суверенних інформаційних ресурсів в умовах активізації сучасних інформаційних взаємовпливів призводить до введення в суспільний обіг несанкціонованої (зокрема, конфіденційної, таємної) інформації. Це не лише негативно впливає на конкурентоспроможність вітчизняних інформаційних ресурсів у сучасному світі, але створює також можливості для введення у сферу суверенних інформаційних ресурсів чужорідної, шкідливої інформації. Одним із характерних прикладів активізації таких процесів є вплив елементів сучасної масової культури на національний культурний процес в умовах глобалізації. Характерна для сучасності глобальна інформаційна експансія також дуже помітно впливає на суверенні інформаційні ресурси на рівні насамперед державному, уніфікуючи їх в інтересах ТНК та провідних у сучасному процесі інформатизації держав.

Загроза техніко-технологічного відставання зумовлює загрози для інформаційного суверенітету під впливом цілої низки негативних чинників. Серед них на сьогодні найбільш відчутним є, як правило, заснована на нових технологічних рішеннях, комп'ютерна злочинність, комп'ютерний тероризм, несанкціоноване проникнення в суверенні масиви інформації, що становлять державну та іншу передбачену законом таємницю, інтелектуальну власність соціальних структур, окремих членів суспільства, а також інформацію, що є власністю держави чи спрямована на забезпечення потреб та інтересів українського суспільства. Як свідчить міжнародна практика, реальними на сьогодні є також загрози, пов'язані зі спробами введення в суверенні інформаційні масиви недостовірної, руйнівної для них інформації.

Причиною сучасної інформаційної експансії дослідники вважають насамперед беззаперечну техніко-технологічну перевагу інформаційної інфраструктури провідних країн-глобалізаторів над можливостями збереження,

використання, виробництва суверенних інформаційних ресурсів у країнах, що потрапили під потужні глобальні інформаційні впливи.

Зазначене вище свідчить, що сучасний науково-технічний прогрес не забезпечує надійного захисту суверенних масивів інформації від зовнішніх впливів навіть при умові високого рівня економічного, техніко-технологічного розвитку, забезпеченого суспільством. Більше того, з розвитком глобального інформаційного простору, процесів інформатизації в усьому світі суверенні масиви інформації ставатимуть все більш вразливими до зовнішніх впливів, традиційні уявлення про забезпечення інформаційного суверенітету ставатимуть все менш ефективними в їх практичній реалізації.

При цьому, все ж основними негативними факторами технічного характеру, що впливають на забезпечення захисту національної інформаційної інфраструктури від кіберзагроз в сучасних умовах, є:

– відставання в розробці і впровадженні нової вітчизняної техніки, програмних продуктів, зокрема спрямованих на нейтралізацію наявних кіберзагроз (програм «антивірус» тощо), інформаційних технологій та недостатнє забезпечення у зв'язку з цим ефективного функціонування інформаційної основи розвитку суспільства;

– повільне впровадження новітніх зарубіжних техніко-технологічних здобутків у процес інформатизації в Україні, використання їх без необхідної в інтересах нашого суспільства адаптації, що негативно впливає на вітчизняний інформаційний суверенітет, безпеку національної інформаційної інфраструктури;

– недостатня участь у міжнародному інформаційному співробітництві, зокрема техніко-технологічному, що на сьогодні є важливим стимулом розвитку науково-технічного прогресу. Налагодження рівноправного співробітництва відповідно до національних інтересів України має сприяти піднесенню технологічного рівня вітчизняної інформаційної діяльності до потреб сучасності, до забезпечення ефективного функціонування національної інформаційної сфери.

Аналізуючи проблему зберігання суверенних інформаційних ресурсів в умовах активізації впливів глобального інформаційного простору, варто звернути увагу на ще одну важливу особливість. Йдеться про значні обсяги високоякісної, створеної і апробованої багатьма поколіннями українського народу інформації на паперових та інших носіях. Саме ця інформація належить переважно до національного надбання, відображає національну специфіку у ставленні до проблем навколишнього світу, є базою для самоідентифікації й основою розвитку національних традицій у науці, культурі, інших сферах суспільної діяльності. Ці пласти вітчизняної інформації зберігаються у фондах бібліотек, архівах, базах та складах даних інших державних та громадських установ. І сьогодні у відповідності із проявленою у світі закономірністю ці фонди оцифровуються, здійснюються заходи до їх широкого уведення у суспільний обіг.

Однак, як свідчить досвід, цей процес, позитивний і необхідний за своєю суттю, має спиратися на добре продуману, виправдану стратегію використання

таких ресурсів. Активізуючи свою діяльність у міжнародних інформаційних обмінах, вітчизняне суспільство не повинно розкривати всі наявні ресурси в інформаційних мережах. Адже навіть при найоптимістичніших сценаріях національна інформаційна інфраструктура не зможе повністю їх захистити від негативних впливів і несанкціонованого запозичення. І тому очевидно, що із розвитком процесів оцифрування необхідно ввести у практику обов'язкове формування баз страхових копій електронної інформації, не пов'язаних постійно діючими лініями зв'язку із системою електронних інформаційних комунікацій. Особливо важливу інформацію при цьому доцільно зберігати також і на неелектронних видах носіїв, на папері, в мікрофільмах тощо. Надійність такого способу захисту особливо важливої інформації можна вважати близькою до 100 %. Національна інформаційна інфраструктура має передбачати наявність центрів такого зберігання інформації, забезпечувати відповідну техніко-технологічну базу.

Паралельно із цією проблемою набула вже значної актуальності необхідність організації безпеки національної інформаційної інфраструктури у сфері забезпечення розвитку інформаційних ринків. Такі ринки, що є на сьогодні найбільш ефективними механізмами інформаційних обмінів, стимулом внутрішньосуспільної циркуляції інформації, ставлять конкретні вимоги до функціонування інформаційної інфраструктури щодо забезпечення захисту інтелектуальних продуктів від несанкціонованого використання, до наявності в ній різноманітних, технологічно сучасних і ефективних форм просування інформаційних продуктів на ринках і, нарешті, до захисту власної інфраструктури від впливів, спрямованих на зниження ефективності її функціонування і можливостей розвитку.

Слід зауважити, що порівняно із розвитком техніко-технологічної бази національної інформаційної інфраструктури інструменти захисту інформаційного суверенітету розвиваються слабо. Більше того, зацікавлені в їх нейтралізації сили вітчизняного і зарубіжного походження під прикриттям боротьби за свободу слова (дуже вразливої для громадської думки на Заході теми і невід'ємного показника західної демократії) ведуть постійну боротьбу проти будь-яких намагань організації відстоювання державних, національних інтересів у розвитку вітчизняного інформаційного простору.

Ще одна причина осучаснення злочинності пов'язана зі стрімким розвитком інформаційних технологій. Вони сприяли виникненню нового виду злочинності – комп'ютерної, а перехід на методи електронного управління технологічними процесами – появі нового виду тероризму –кібертероризму. Кібертероризм – це різновид тероризму, в основу якого покладено спосіб здійснення терористичних дій, що виник у процесі розвитку інформаційно-телекомунікаційних технологій та впровадження їх у всі сфери сучасного суспільства [7]. На думку С. Хоффмана, міжнародний тероризм виявився можливим завдяки широкому набору засобів комунікації [8].

Актуальність проблеми кібертероризму для України подвійна: з одного боку, держава не настільки багата, щоб переобладнати сучасними засобами управління свої хімічні підприємства, атомні електростанції та інші критичні

й уразливі структури, що зробило б їх невразливими для нападу кібертерористів. З іншого, – формування нової інформаційної інфраструктури, вітчизняної системи баз суверенної інформації стає стратегічним ресурсом, який вимагає постійної уваги з боку держави.

Варто зазначити, що у швидкоплинному перебігу подій суспільного життя, з революційними процесами у розвитку інформаційних технологій значна частина чинних нормативних актів як внутрішньодержавних, так і міжнародних поступово втрачає актуальність, відповідність процесам, які ними нормуються, і потребує уточнень або ж перегляду. Розвиток інформаційної діяльності створює необхідність правового урегулювання нових аспектів цієї діяльності. Потребує досконалого правового обґрунтування питання організації ефективного протистояння кібертероризму в умовах активізації глобальних впливів, нових інформаційних технологій. Комплекс відповідних правових актів має постійно вдосконалюватися із урахуванням відповідного міжнародного законодавства, його еволюції і вітчизняної законотворчої практики, що має бути на варті інтересів національної інформаційної діяльності.

Оскільки процес протидії сучасним кіберзагрозам – явище багатоаспектне і належить до категорії життєво необхідних, в умовах переходу до інформаційного суспільства, цей процес має спиратися на комплексну систему організаційних заходів. Серед них найбільш актуальним є організація ефективної роботи загальноукраїнського центру аналізу інформаційних, зокрема і кіберзагроз, координації роботи з їх нейтралізації. Такий координаційний центр має організовувати відстежування загроз, вивчення тенденцій їх розвитку, значення їх реального і потенційного впливу на інформаційну структуру, забезпечувати прогноз розвитку ситуації і розробку змісту заходів на попередження. Він повинен мати можливості для ефективного залучення до справи боротьби з кібертероризмом відповідні державні установи, приватні економічні структури, що спеціалізуються на проблемах охоронної діяльності, громадські співтовариства протидії негативним впливам на діяльність інформаційної сфери, надавати суспільно важливу інформацію із цього питання для ЗМІ.

Невпорядкованість процесу доступу до мережі Інтернет державних органів, підприємств, установ та організацій, які отримують, обробляють, поширюють і зберігають інформацію з обмеженим доступом, створює умови для розміщення державних Інтернет-ресурсів на технічних майданчиках, які не мають відповідного рівня захищеності, особливо це характерно для органів місцевого самоврядування [9].

У зв'язку з цим першочерговим питанням є формування організаційно-правових засад побудови системи захисту критичної інфраструктури від кібернетичних атак. Її завданнями мають бути визначення об'єктів вітчизняної інфраструктури, що потребують першочергового захисту від кібернетичних загроз з урахуванням іноземного досвіду, визначення критеріїв їх віднесення, класифікація за категоріями, обґрунтування пропозицій щодо законодавчого регламентування захисту вітчизняної інфраструктури від протиправних кібернетичних посягань.

Сьогодні багато елементів критичної інфраструктури держави знаходяться у сфері володіння приватного сектору і не є державною власністю. Тому вкрай важливим моментом в організації системи забезпечення безпеки держави є створення відповідної системи координації, до складу якої б входили як урядові, так і громадські організації із залученням комерційних структур, які працюють у ключових секторах критичної інфраструктури держави. Тісний взаємозв'язок між державним і приватним сектором країни є невід'ємною умовою безпеки держави [10].

Однозначного наукового визначення потребує термінологія у сфері забезпечення кібернетичної безпеки, зокрема поняття «критична інфраструктура». При цьому вітчизняні та зарубіжні науковці мають різні підходи до визначення цього поняття. Так, більшість науковців відносять до такої інфраструктури всі інформаційні системи, що безпосередньо здійснюють управління державою та економікою. Проте, прихильники іншого підходу визначають дефініції «інформаційна інфраструктура» як сукупність мереж, основне призначення яких передача інформації із змістовим навантаженням (телерадіомережі, засоби масової інформації, телекомунікаційні мережі всіх видів) та «критична інфраструктура» як сукупність мереж, основне призначення яких передача технологічної інформації з метою управління технологічними процесами виробництва чи надання послуг (інформація не має змістового навантаження).

З огляду на те, що кібератаки зазнають постійних змін, їх складно прогнозувати та відстежувати у реальному часі, гостро постає питання вдосконалення системи забезпечення інформаційної безпеки. Досягнення поставленої мети потребує наукового опрацювання та подальшого супроводження таких напрямів, як: розвиток захищених телекомунікаційних систем; підвищення надійності спеціального програмного забезпечення; розробка адекватних методів контролю ефективності засобів захисту інформації; виявлення технічних пристроїв і програм, що становлять небезпеку для штатного функціонування інформаційно-телекомунікаційних систем; запобігання перехопленню інформації технічними каналами; формування системи моніторингу показників якості захисту інформації тощо.

Стрімкий розвиток в Україні інформаційних технологій та інтеграція нашої держави до світового інформаційного простору створює передумови для реалізації кіберзагроз аналогічного характеру щодо вітчизняної інфраструктури.

Висновки. Організація безпеки сучасної інформаційної інфраструктури, що перебуває в постійному розвитку, якісно змінюється під впливом прискорених темпів науково-технологічного прогресу, зумовлює необхідність відповідного забезпечення на всіх інших етапах виробництва, організації зберігання та використання інформаційних ресурсів.

Проблема розробки і вибору ефективних методів і засобів захисту інформаційної інфраструктури ґрунтується на комплексному підході та має такі складові:

– правову – пов'язана з розробленням нормативно-правових актів, які регламентують відносини в інформаційній сфері, і нормативно-методичних документів із питань забезпечення інформаційної безпеки;

– організаційну – полягає в удосконаленні організаційної структури державних і комерційних підприємств, сертифікації і стандартизації засобів захисту інформації та ліцензуванні діяльності у сфері захисту інформації;

– психологічну – передбачає формування морально-етичних норм у співробітників, які працюють з інформаційними системами, що забезпечують критичну інфраструктуру держави;

– технічну – ґрунтується на створенні і постійному вдосконаленні системи забезпечення інформаційної безпеки на об'єктах інформатизації та попередження нападу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

2. *Онищенко О.С.* Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій / О.С. Онищенко, В.М. Горовий, В.І. Попик; [та ін.]. – Київ : Нац. б-ка України ім. В.І. Вернадського, 2011 . – С. 64.

3. Ministry of Information and Communication (MIC). – Mode of access: http://www.mic.go.kr/eng/jsp/main.jsp; Korean Broadcasting Commission. – Mode of access: http://www.kbc.or.kr/english/index.html; Korea National Statistical Office. – Mode of access: http://www.nso.go.kr/eng; Korea Network Information Center. – Mode of access: http://www.nic.or.kr/www/english/index.html.

4. Information Superhighway: An Overview of Technology Challenges: Report to the USA Congress, 1995. – Mode of access: http://www.eric.ed.gov/ERICWebPortal/search/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=ED380136&ERICExtSearch_SearchType_0=no&accno=ED380136.

5. Building the Information Society: Moving Canada into the 21st Century / Ministry of Supply and Services, Canada, 1996.

6. World Economic Forum, The Global Information Technology Report 2010–2011. – Mode of access: http://www.weforum.org/reports.

7. *Голубєв В.О.* Інформаційна безпека: проблеми боротьби з кіберзлочинами: моногр. / В.О.Голубєв. – Запоріжжя: ГУ «ЗІДМУ», 2003. – 250 с.; *Старостина Е.* Терроризм и кибертерроризм – новая угроза международной безопасности [Электронный ресурс] / Е.Старостина. – Режим доступу: http://www.crime–research.ru/articles/starostina.

8. *Хоффман С.* Столкновение глобализаций: Как сделать мир более пригодным для жизни. Новая парадигма? [Электронный ресурс] / Хоффман С. – Режим доступа: http//www.imperativ.net/imp11/Hoffman.html

9. *Петров В.* Стан захищеності інформаційних ресурсів України та шляхи її вдосконалення /В.Петров// Актуальні проблеми міжнародної безпеки: український вимір. – К. : ВД «Стилос», 2010. – С. 577.

10. *Сайтарли Т.* Захист критичної інфраструктури – складова частина національної безпеки і стабільності [Електронний ресурс] / Т.Сайтарли. – Режим доступу: http://www.crime–research.ru/library/Saytarly aprl.htm.

Довгань О.Д. Сучасна інформаційна інфраструктура України і основні завдання щодо її захисту

У статті роглянуті інформаційна інфраструктура України і основні завдання по її захисту в умовах сучасних глобалізаційних процесів і стрімкого розвитку інформаційних технологій.

Ключові слова: *інформаційна інфраструктура, інформаційні ресурси, критична інфраструктура, кібертероризм.*

Довгань А.Д. Современная информационная инфраструктура Украины и основные задания ее защиты

В статье рассмотрена информационная инфраструктура Украины и основные задания по ее защите в условиях современных глобализационных процессов и стремительного развития информационных технологий.

Ключевые слова: *информационная инфраструктура, информационные ресурсы, критическая инфраструктура, кибертерроризм.*

Dovgan O. Modern information infrastructure of Ukraine and basic tasks of its protection

The article considers information infrastructure of Ukraine and main problems of its protection in modern processes of globalization and information technologies development.

Keywords: *information infrastructure, information resources, critical infrastructure, cyberterrorism.*

Стаття надійшла до редакції 19.05.2015.