Русскіх М.*

ПОЛІТИКА США В СФЕРІ КІБЕРБЕЗПЕКИ

З масовим поширенням кожного нового покоління інформаційно-комунікаційних технологій відповідно зростає рівень їхнього використання урядом Сполучених Штатів Америки. Державні та місцеві органи влади використовують технології нового покоління для більш ефективного виконання повсякденних адміністративних функцій, для вдосконалення роботи державних відомств та служб, для доступу до урядової інформації. Федеральний уряд Сполучених Штатів впровадив еволюційні ІКТ також і для виконання важливих державних функцій, таких як діяльність у галузі зовнішніх зносин, військового командування та управління, зовнішньої розвідки.

Директива по забезпеченню національної безпеки №54 (National Security Presidential Directive 54 – NSPD-54), та директива по забезпеченню внутрішньої безпеки №23 (Homeland Security Presidential Directive 23 – HSPD-23) видані колишнім президентом США Дж. Бушем, визначають поняття «кіберпростір» як незалежну мережу інформаційних технологій та інфраструктури, яка включає в себе Інтернет, телекомунікаційні мережі, комп'ютерні системи, а також вбудовані процесори і контролери у важливих галузях промисловості. Глобально взаємопов'язана цифрова інформаційна та комунікаційна інфраструктура – кіберпростір – підтримує практично кожний аспект сучасного суспільства, а також є важливим фундаментом для економіки США, громадської інфраструктури, безпеки громадян, а також національної безпеки [1].

У доповіді комісії з кібербезпеки США, створеної після серії атак на мережі Пентагону в 2007-2008 році, проголошеної у грудні 2008 року чітко зазначено: «Неспроможність Сполучених Штатів захистити кіберпростір є однією з найважливіших проблем національної безпеки держави, з якою зіштовхнеться нова адміністрація президента» [2]. Загрози кіберпростору є однією з найважливіших викликів економічній та національній безпеці Сполучених Штатів в цілому. Населення, торгівля, життєво важлива інфраструктура, а також уряд США є своєрідними «мішенями» для зростаючої кількості державних та недержавних суб'єктів, таких як терористичні угрупування, міжнародні злочинні угрупування. Ці суб'єкти мають можливість піддавати небезпеці, красти, змінювати, або повністю знищувати інформацію. Як нещодавно зазначив керівник національної розвідки Сполучних Штатів, «зростаюча взаємопов'язаність інформаційних систем, Інтернету та іншої інфраструктури створює можливості для хакерів руйнувати телекомунікаційні мережі, лінії електропередач, нафтопереробні пристрої, фінансові мережі та іншу життєво важливу інфраструктуру». Урядові органи розвідки США оцінюють, що вже існує ряд держав, які мають технологічну спроможність наносити такі атаки [1].

Президентські директиви Дж. Буша NSPD-54 та HSPD-23, видані 8 січня 2008 року поклали початок комплексу заходів по захисту кіберпростору США, які проводяться теперішньою адміністрацією Вашингтона. Саме тоді починання екс-президента у галузі кібербезпеки отримали назву Комплексної національної ініціативи забезпечення

* студентка 4 курсу спеціальності «міжнародна інформація» Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Науковий керівник: доц. Андрєєва О.М.

кібербезпеки (The Comprehensive National Cybersecurity Initiative – CNCI). Тоді до громадськості були донесені лише загальні напрями діяльності по розробці цієї програми, вона мала гриф «секретно». Проте у вересні 2010 року громадяни США отримали можливість ознайомитися з попередньо закритими положеннями CNCI на сайті Ради національної безпеки, де були опубліковані 12 напрямів діяльності федеральних відомств Сполучених Штатів, відповідальних за забезпечення захисту інформаційних мереж [3]. Основна ціль CNCI полягає в укріпленні правопорядку, розвідки, контррозвідки та військового потенціалу для вирішення повного спектру кіберзагроз [4]. Донесення до громадськості національної ініціативи забезпечення кібербезпеки Вашингтону в області кібербезпеки було здійснено відповідно до меморандуму про відкритість і прозорість американського уряду, виданий Президентом США Б. Обамою на початку 2010 року.

Одразу після вступу на посаду Президента США, Б. Обама видав наказ про проведення ретельного аналізу заходів, що проводяться відповідальними федеральними структурами з організації ефективного захисту національної інфраструктури зв'язку і передачі даних, і про розробку комплексного підходу до забезпечення надійного захисту кіберпростору США [3].

Заявляючи, що хакери є однією з головних загроз економічній та національній безпеці США, 29 травня 2009 року Президент США Б. Обама заявив про створення в Білому Домі відділу з кібербезпеки, очолювати який доручив «кіберцарю», обов'язки якого передбачають координацію роботи урядових агентств та зусиль по забезпеченню інформаційної безпеки. «Кіберцар» має звітуватися перед Радою національної безпеки та Економічною радою, а також регулярно звітуватися президенту [5].

Усвідомлюючи виклики, що представляють собою кібератаки, Президент США визначив забезпечення кібербезпеки як одне з пріоритетних завдань його адміністрації. З метою забезпечення стійкості, надійності, та захищеності кіберпростору для підтримки цілей економічного зростання, захисту громадянських свобод та прав на приватне життя, національної безпеки та постійного удосконалення демократичних інститутів, кібербезпека має увійти в ряд першочергових національних пріоритетних завдань. Виконання цього важливого і складного завдання можливе лише за умови ефективного керівництва на найвищому урядовому рівні. Адміністрація вже створила Міжвідомчий комітет, що проводить політику з питань інформаційно-комунікаційної інфраструктури (Information and Communications infrastructure Interagency Policy Committee (ICI-IPC), який очолює Рада національної безпеки та Рада внутрішньої безпеки США, в якості основного органу, що координує політику з питань, що стосуються створення надійної та безпечної глобальної інформаційної та комунікаційної інфраструктури та пов'язаних з нею можливостей [1].

Відповідно до рекомендацій фахівців, викладених у звіті «Огляд політики у кіберпросторі» за вказівкою президента, нова адміністративна структура Білого дому повинна співпрацювати з усіма провідними федеральними відомствами, що відповідають за забезпечення безпеки систем і засобів національної інформаційної інфраструктури. Вони також зобов'язані безперервно взаємодіяти з урядами штатів, керівництвом органів місцевого управління та відповідними підрозділами приватних фірм, які забезпечують захист закритих корпоративних даних [3].

США потребують всеохоплюючу структурну схему, яка буде сприяти чітким та скоординованим відповідям уряду та приватного сектору на серйозні кібератаки. Федеральний уряд, державний, та місцеві уряди мають удосконалювати свої плани та ресурси, направлені на те щоб виявити, попередити, та відповісти на серйозні кібератаки. Оскільки кібератаки впливають на взаємопов'язані мережі як урядові, так і промислові,

координація планів та ресурсів уряду та промислового сектору є важливою до, під час, та після серйозних атак.

Література

1. Cyberspace Policy Review [Електронний ресурс] / National Security Council – Режим доступу до ресурсу: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
2. Securing Cyberspace for the 44th Presidency [Електронний ресурс] / A Report of the CSIS Commission on Cybersecurity for the 44th Presidency / Washington, DC – 2008 – Режим доступу до ресурсу: csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
3. США продолжают созидать киберстену [Електронний ресурс] / В.Иванов // Независимое военное обозрение – 2010-04-09 – Режим доступу до ресурсу: http://nvo.ng.ru/spforces/2010-04-09/15_cyberwall.html
4. Cyberspace Policy Review – 2009 «The cyberSpace Race» [Електронний ресурс] / Southern Virginia Security cyWar Stories – 06.06.2009 – Режим доступу до ресурсу: http://www.sovasec.com/tag/ici-ipc/
5. «Барак Обама учредил в Белом доме должность «киберцаря» [Електронний ресурс] / Information Security – 01.06.2009 – Режим доступу до ресурсу: http://www.itsec.ru/newstext.php?news_id=58330