Медведєва О.*

КІБЕРПРОСТІР ЯК СФЕРА ДІЯЛЬНОСТІ РОЗВІДУВАЛЬНИХ СЛУЖБ

1. З означенням нових джерел загроз - в тому числі для національних інтересів окремих держав - робота розвідувальних служб набуває особливого значення. Будь-яка держава, яка претендує на роль вагомого актора на міжнародній арені, потребує сучасної, належно оснащеної, висококласної розвідки, діяльність якої створює умови для надійного захисту національних інтересів у непростих жорстких конкурентних умовах сучасних міжнародних відносин.

2. Незважаючи на зміщення людства загалом у бік інформаційної цивілізації, функції розвідувальних служб не зазнали суттєвих змін. Проте в ході глобальної інформатизації виникло принципово нове середовище протиборства розвідувальних служб конкуруючих держав - кіберпростір, що зумовлює особливості діяльності розвідки у XXI столітті. Провідними державами світу питання кібербезпеки виноситься на найвищий рівень. Про це свідчить створення у Пентагоні нового командування – кібернетичного. Відповідний наказ у 2009 році підписав міністр оборони США Роберт Гейтс. Ще одним доказом є заснування восени 2000 року аналогічної структури в Японії. Створення так званих «кібервійськ» означає офіційне визнання урядами необхідності захищати свої інформаційні ресурси від зовнішніх загроз і бути готовими адекватно відповісти на напад з кіберпростору або на загрозу такого нападу. Таким чином, можна стверджувати про створення нового роду військ про оснащення їх спеціальними системами озброєння і військової техніки [1].

3. Принципово новий підхід до діяльності розвідувальних служб США зумовлений тим, що 95% ліній зв'язку комп'ютерних мереж Міністерства оборони США розгорнуто на базі загальнодоступних телефонних каналів, а понад 150 тисяч комп'ютерів підключені до мережі Інтернет, що робить їх надзвичайно вразливими. Весь стандартизований комп'ютерний комплекс може бути швидко виведений з ладу атакою, орієнтованою на спільний для стандартизованої мережі вразливий елемент - наприклад, операційну систему або протокол зв'язку. Зазначена обставина може бути ефективно використана радіоелектронною розвідкою країни-розробника цих уніфікованих платформ. Виходячи з цього, ЦРУ і військова розвідка США вивчають можливості і методи проникнення в комп'ютерні мережі своїх потенційних супротивників. Для цього розробляються технології впровадження електронних вірусів і «логічних бомб», які здатні активізуватися по команді. Це дає можливість дезорганізувати оборонну систему управління, транспорт, енергетику, фінансову систему іншої держави. Ефективними для досягнення зазначених цілей можуть стати «заражені» мікросхеми після їх впровадження у експортовану Сполученими Штатами обчислювальну техніку[2].

4. Еволюція розвідувальних служб як відповідь на загрози нового інформаційного суспільства відбувається в багатьох розвинутих державах. Так, наприклад, командування

* студентка 3 курсу спеціальності «міжнародна інформація» Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка
Науковий керівник: доц. Даниленко С.І.

збройних сил Німеччини приступило до створення служби мережевих операцій з конкретною метою - здійснення впливу на комп'ютерні мережі противника, яке спрямоване на використання, спотворення, підміну або знищення інформації, що міститься в базах даних комп'ютерів та інформаційних мережах, а також зниження ефективності їх функціонування або виведення з ладу. У ФРН було припинено спробу проникнення в бази даних німецького уряду з міст Ланьчжоу, Кантон і Пекін. При цьому з метою маскування хакери діяли через проміжний сервер мережі Інтернет в Південній Кореї. Для проникнення в урядову мережу ФРН зловмисники встановили прихований контроль за сайтом Powerpoint у Всесвітній павутині. При заході на ці сайти з персонального комп'ютера будь-якого урядового об'єкта цей комп'ютер заражаються вірусом, який пізніше міг проникнути у внутрішню мережу установи [3].

5. Необхідність виходу на новий рівень захисту і боротьби у кіберпросторі вплинула на китайські розвідувальні служби, які не відстають від західних демократій і активно освоюють кіберпростір. Про це свідчить виявлення канадськими вченими мережі електронних шпигунів, розташованих переважно в Китаї, що відстежують вміст комп'ютерів, які розміщені в урядових установах по всьому світу. За словами вчених з Університету Торонто, вірус-шпигун відстежував вміст 1295 комп'ютерів у 103 країнах. [4].

6. Отже, у XXI столітті кіберпростір являє собою одну з ключових сфер, контроль над якою дозволить в найближчому майбутньому підтримувати військову перевагу над противниками, і у зв'язку з цим необхідними є зусилля держав в напрямку створення відповідного кібернетичного потенціалу. Поява нових загроз породила необхідність контролю та регулювання кіберпростору розвідувальними службами. Саме це стало головною причиною того, що сьогодні могутні держави активно займаються розробкою інформаційної зброї. Провідні країни світу розширюють і створюють у збройних силах і спецслужбах підрозділи, які повинні забезпечити розвиток наступальних можливостей в кіберпросторі. Це дозволяє говорити про початок так званої гонки озброєнь в кіберпросторі.

Список використаної літератури:

1. Бойцы виртуального фронта [Електронний ресурс]. – Режим доступу: http://www.vremya.ru/2009/110/72/231942.html
2. Димлевич Н. R-Techno: Об использовании информационного оружия в киберпространстве [Електронний ресурс]/ Димлевич Николай. – Режим доступу: http://it2b-forum.ru/index.php?showtopic=12576
3. Киберпространство в XXI столетии: новые угрозы. [Електронний ресурс]. – Режим доступу: http://sites.google.com/site/zadumajtes/goracie-tocki/amerika/ kiberprostranstvo-v-xxi-stoletii-novye-ugrozy
4. Китайський привид у комп'ютері? [Електронний ресурс]. – Режим доступу: http://www.zgroup.com.ua/article.php?articleid=2355