Матвєєв А.*

ПОЛІТИКА КІБЕРБЕЗПЕКИ США НА СУЧАСНОМУ ЕТАПІ

На сучасному етапі під поняттям «кібервійна» (англ. Cyber-warfare) розуміють комп'ютерне протистояння у просторі Інтернету.

Не варто плутати це поняття з мережевою війною — котра ведеться використовуючи мережеві технології (це не тільки Інтернет)..

Кібервійна спрямована передусім на дестабілізацію комп'ютерних систем і доступу до Інтернету державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країн, які покладаються на Інтернет у повсякденному житті. Міждержавні стосунки і політичне протистояння часто знаходить продовження в Інтернеті у вигляді кібервійни: вандалізмі, пропаганді, шпигунстві, та безпосередніх атаках на комп'ютерні системи та сервери.

Як визначив експерт з безпеки уряду США Річард А. Кларк, в своїй книзі «Кібервійна» (англ. CyberWarfare) (вийшла в травні 2010) «кібервійна — дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування». Американський журнал Економіст (англ. The Economist) описує кібервійну як «п'яту область війни, після землі, моря, повітря і космосу». Про важливість готовності до ведення військових дій в кіберпросторі свідчить факт створення в США цілого військового підрозділу — Кіберкомандування США.

На сьогоднішній день спеціалісти виділяють такі види атак в Інтернеті:

- Вандалізм — використання хакерами Інтернету для паплюження інтернет сторінок, заміни змісту образливими чи пропагандистськими зображеннями.
- Пропаганда — розсилка звернень пропагандистського характеру, або вставка пропаганди в зміст інших інтернет сторінок.
- Збір інформації — зламування приватних сторінок чи серверів для збору секретної інформації чи її заміни на фальшиву, корисну іншій державі.
- Відмова сервісу — атаки з різних комп'ютерів для унеможливлення функціонування сайтів чи комп'ютерних систем.
- Втручання в роботу обладнання — атаки на комп'ютери, які займаються контролем над роботою цивільного чи військового обладнання, що призводить до його відключення чи поламки.
- Атаки на пункти інфраструктури — атаки на комп'ютери, які забезпечують життєдіяльність міст, їх інфраструктури, таких як телефонні системи, водопостачання, електроенергії, пожежної охорони, транспорту, тощо

На відміну від кібератак минулого, зараз кібервійна являє собою реальну загрозу для національної безпеки країн і сприймається багатьма як серйозна загроза безпеці держави.

Крім того, розвідувальні організації багатьох країн займаються шпигунством використовуючи Інтернет: збирають інформацію, зламують комп'ютерні системи інших держав, займаються диверсійною діяльністю та економічним шпигунством. За визнанням

* студент 2 курсу спеціальності «міжнародна інформація» Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

спеціалістів, лідерами у веденні кібервійни зараз є Китай та Росія. Зокрема Китай звинувачували у організації атак на сайти Сполучених Штатів, Німеччини, Індії. Росія використовує Інтернет не тільки для збору інформації, але й для організації масованих атак на недружні країни. Росія, як і Китай, однак, заперечують причетність державних установ до організації атак.

Беруть участь у кібервійнах і українські хакери. Так після подій навколо акту вандалізму на Говерлі, сайти Євразійського союзу молоді, який взяв відповідальність за їхнє проведення, були атаковані з України. У відповідь зазнали атак сайти президента України та СБУ.

В зв'язку з розвитком нових технологій рівень кібервійни постійно вдосконалюється. Деякі держави починають приділяти захистові від кібервійни належну увагу — виділяють необхідні кошти для організації систем захисту і підтримують спеціальні підрозділи, основною задачею яких є вдосконалення інтернетної безпеки країни та захисту від нападів.

Було розроблено декілька проектів міжнародних конвенцій з приводу заборони кібервійни. Наприклад, професор Олександр Мережко розробив проект міжнародної угоди, який називається «Конвенція про заборону використання кібервійни в глобальній інформаційній мережі інформаційних і обчислювальних ресурсів (Інтернеті)». Згідно його проекту, Інтернет повинен залишитися вільним від військових дій і розглядатися як «спільна спадщина людства»

США також не стоїть осторонь у вирішені цього питання. Так, Адміністрація нинішнього президента США Барака Обами планує створення нового військового командування, в завдання якого ввійде координація захисних програм Пентагону, ЦРУ і спецслужб США, пов'язаних з комп'ютерними і мережевими системами. Нова ініціатива, кажуть військові експерти, повинна буде з одного боку підвищити захищеність державних мереж, а з іншого модернізувати нинішні системи, які не мають єдиного центру.

Однією з головних завдань центру кіберкомандування є протистояння атакам хакерів, що йде, в першу чергу, з території Китаю і Росії.

Раніше Обама проголосив кібербезпеку США одним із пріоритетів своєї політики. У новій Адміністрації кажуть, що розглядають кібербезпеку невідривно від загальної внутрішньої безпеки США. Барак Обама також запланував проведення низки дослідницьких робіт, пов'язаних зі створенням нового покоління засобів для забезпечення безпеки серверів і мереж, які обслуговують найважливіші державні вузли. Окремо в плані наголошується на необхідність боротьби з кібершпіонажем і кібершахрайством, які в останні пару років стали перманентним явищем.

У Вашингтоні був представлений попередній варіант документа, що регламентує стандарти і заходи безпеки з охорони цифрових даних, а також процедур, що регулюють їх розкриття. Юристи відзначають, що цей документ має на меті створення законодавчої бази для судового переслідування хакерів.

«Ми всі знаємо, що кібершпіонаж і мережеві злочини стали наростаючою тенденцією. Такі країни, як Китай швидко вловили цю зміну. В останні 8 років ми [США] запізнилися в цьому», - сказав Обама. «Як президент, я зроблю кібербезпеку вищим пріоритетом, який повинен бути в 21 столітті».

Але підсумковий масштабний документ, що регламентує центр кіберкомандування, поки не узгоджений до кінця. Немає ясності з низки ключових питань, зокрема щодо взаємодії з приватними структурами, особливо тими, що працюють у сфері телекомунікацій та енергопостачання. За непідтвердженими даними, в документі передбачається досить широка програма взаємодії не тільки з приватними комерційними структурами, а й з громадськими, некомерційними і правозахисними структурами.

Також відомо, що поки в документі немає єдиного погляду на роль держави в новій доктрині кібербезпеки. WSJ (wall street journal), посилаючись на свої джерела в уряді США, пише, що про створення центру кіберкомандування оголосить Міністр оборони США Роберт Гейтс, але буде це лише після того, як Білий Дім затвердить всі аспекти проекту.

На сьогодні в США є кілька організацій, що відповідають за ІТ-безпеку військових та урядових мереж. Так, Штаб центрального командування відповідає за ІТ-безпеку військових в Іраку і Афганістані, Командування центральних операцій відповідає за безпеку елітних військових підрозділів, свої центри безпеки є також у ВПС і ВМФ США. Всі вищеперераховані структури між собою не пов'язані.

Що стосується нової ІТ-структури, то її, за попередніми даними, очолить директор АНБ США Кейт Олександр, що знаходиться в званні Генерала армії США. Таким чином, АНБ буде відповідати за кібербезпеку всього Міноборони США та урядових мереж.

Білий Дім у Вашингтоні напередодні запропонував ряд законодавчих актів, що дозволяють захищати США від кібератак хакерів, шахраїв і шпигунів, говориться в офіційних документах, опублікованих напередодні на сайті Адміністрації президента США.

Відповідно до запропонованого плану, раніше підтриманого президентом країни Бараком Обамою, американські компанії, в управлінні яких знаходяться об'єкти критично важливої інфраструктури повинні будуть співпрацювати з урядовими органами, щоб обидві сторони були переконані у надійності критично важливих інфраструктур. До таких важливих об'єктів в законодавчих актах відносять електро-і атомні станції, комп'ютерні мережі банків і бірж, об'єкти комунального господарства, наприклад міські системи водо- і газо-постачання та інші.

За новими пропозиціями, які отримали неофіційну назву CyberAct, Департамент Національної безпеки США отримує право вимагати від цих компаній виконання тих чи інших додаткових норм з промислової безпеки.

Напередодні в Білому домі та Конгресі США одночасно заявили, що урядові і приватні ІТ-системи в США піддаються хакерським нападам приблизно по мільйону раз на день. Скільки нападів обертаються крадіжкою даних - невідомо.

Аналітики кажуть, що в першу чергу новий план призначений для боротьби з промисловим шпигунством з боку іноземних держав. У США кажуть, що за останні 3-4 року мережі бірж, промислових компаній, ресурси високотехнологічних виробників стали регулярно піддаватися атакам хакерів, масштаби і складність яких постійно зростають.

Пропозиція Білого дому в першу чергу передбачає, щоб Департамент Національної безпеки виробив додаткові норми для фінансових компаній та енергетичного сектора. Також в оцінці створених систем безпеки планується залучити незалежних ІТ-аудиторів.

У середовищі американських бізнесменів дана програма здебільшого не знаходить підтримки, так як більшість компаній заявляють, що вважають за краще добровільні програми, а не нав'язані з боку держави. В Адміністрації Барака Обами кажуть, що в якості остаточного закону пропозиція повинна бути оформлено до кінця року.

Отже, з поширенням комп'ютерних технологій та Інтернету багато громадян, підприємств і державних установ почали залежати від Інтернет-зв'язку у повсякденному житті. Використання Інтернету для атак комп'ютерних систем іншої держави може завдати значної шкоди її економіці і створити розлад у повсякденному житті країни. Тож в наш час поняття кібербезпеки та кібервійни набувають нової значимості, а важливість інформаційної безпеки переходить на зовсім новий рівень. Ця сфера починає потребувати більш чіткого та свідомого регулювання на всіх рівнях. Не зважаючи на значну складність ре-

гуляції діяльності цієї сфери, відбуваються досить вдалі спроби вирішення цього питання на державному рівні, створюються проекти міжнародних документів.

Список використаних джерел:

1. А. А. Мережко «Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете)» [Електронний ресурс] Режим доступу - http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57
2. Clarke, Richard A. Cyber War, HarperCollins (2010)
3. «Хакери з ЄСМ заявляють, що слідом за сайтом Ющенка «положать» сайт СБУ« [Електронний ресурс] Режим доступу - http://www.unian.net/ukr/news/news-219388.html
4. «На Пентагон була здійснена потужна кібератака з Росії» [Електронний ресурс] Режим доступу - http://ua.korrespondent.net/tech/661524-na-pentagon-bula-zdijsnena-potuzhna-kiberataka-z-rosiyi
5. «Світ охопила кібервійна» - [Електронний ресурс] Режим доступу - http://ua.for-ua.com/fun/2007/11/29/140857.html