Сербіна К.*

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА МІЖНАРОДНІЙ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Перехід на методи електронного управління технологічними процесам дає підстави для появи принципово нового виду тероризму – кібертероризму: втручання в роботу компонентів телекомунікаційних мереж, які функціонують у середовищі комп'ютерних програм чи несанкціонована модифікація комп'ютерних даних, яка викликає дезорганізацію роботи критично важливих елементів інфраструктури держави і створює небезпеку загибелі людей, спричинює настання значної майнової шкоди чи інших суспільно небезпечних наслідків.

Трагічні події 11 вересня 2001 року в США переконливо довели органічний взаємозв'язок і неподільність національної, регіональної та глобальної безпеки в умовах сучасної цивілізації. Відбулася не стільки зміна пріоритетів безпеки, скільки нове розуміння підходів до її забезпечення, так як світ опинився на порозі нової доби – доби зміни уявлень про вирішальні можливості держави в забезпеченні сталого розвитку суспільства та безпеки громадян.

Наприкінці XX – на початку XXI століття змінюються погляди на головний суб'єкт і об'єкт безпеки. Якщо раніше головним об'єктом захисту були територія, кордони, державний устрій, людські і матеріальні ресурси суверенної держави, а вона перебирала на себе виконання цих завдань шляхом створення та утримання силових структур (була головним суб'єктом безпеки), то зараз удари терористів спрямовані на мирне населення та інфраструктуру, а існуючі силові структури від самого початку не були призначені для боротьби з новими загрозами (збройні конфлікти всередині держав на етнічному, релігійному або політичному підґрунті; міжнародний тероризм; нелегальне поширення наркотиків і зброї; неконтрольована міграція; «інформаційні війни», які впливають на регіональну та глобальну безпеку і є тіньовою стороною глобалізації світових процесів).

Інформація, що відіграє вирішальну роль у функціонуванні структур державної влади, національної безпеки, суспільних інститутів, стає найслабшим ланцюгом національної інфраструктури держави на сучасному етапі. Глобалізація сучасної економіки, її насиченість новітніми інформаційно-телекомунікаційними технологіями, інформатизація таких життєво вважливих сфер діяльності суспільства, як зв'язок, енергетика, транспорт, системи збереження та транспортування газу та нафти, фінансова і банківська системи, водопостачання, оборона й національна безпека, структури забезпечення роботи міністерств і відомств, єдина служба часу й еталонних частот, перехід на методи електронного управління технологічними процесами у виробництві, є основою для все більшого розповсюдження кібертероризму.

Кібертероризм – це явище міжнародного значення, рівень якого знаходиться у прямій залежності від рівня розвитку та впровадження сучасних комп'ютерних технологій та доступу до них.

---

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

Науковий керівник: доц. Андрєєва О.М.

Власне природа кіберзлочинів робить проблему всесвітньою, оскільки почасти не має значення, де саме вчинено подібний злочин.

Терористичні організації все частіше використовують нові інформаційні технології та Internet із злочинними намірами поповнення коштів, здійснення пропаганди або передачі секретної інформації. Хоча терористи ще не застосовували кіберзброю за призначенням, однак вони використовують нові інформаційні технології і досягнення комп'ютерного прогресу, а це вже сигнал про небезпеку. Кібертероризм, під яким розуміється використання сучасних інформаційних технологій, насамперед мережі Internet, коли така зброя застосовується з метою пошкодження важливих державних інфраструктур (таких, як енергетична, транспортна, урядова тощо), може у недалекому майбутньому стати реальною загрозою для інформаційної безпеки в першу чергу розвинутих країн світу.

У світовому кіберпросторі вже давно здійснюються спецоперації і фактично йде неоголошена інформаційна війна.

На початку XXI століття світ увійшов у період руйнівних війн у кібепросторі майже непідготовленим, оскільки в Internet немає системи міжнародної безпеки, міжнародних договорів або структур, здатних зупинити його мілітаризацію чи хоча б не допустити масштабного використання військової сили. Водночас Internet дедалі частіше використовують з метою психологічного та економічного тиску на опонента.

Новий антитерористичний закон США, відомий як «Акт 2001 року», прийнятий Конгресом через шість тижнів після терористичних атак на Нью-Йорк і Вашингтон. Після його прийняття генеральний прокурор США Джон Ешкрофт зробив заяву для преси: «Новим законом Конгрес ввів у дію деякі нові поняття, що розширюють трактування терміна «тероризм» та створив нове законодавче поняття «кібертероризм» і відніс до нього різні кваліфіковані форми хакерства і спричинення шкоди захищеним комп'ютерним мережам громадян, юридичних осіб і державних відомств, включаючи збиток, спричинений комп'ютерній системі, що використовується державним закладом при організації національної оборони або забезпеченні національної безпеки».

Британський «Закон про тероризм» 2000 р. вважає терористичними дії осіб, які «серйозно порушують роботу будь-якої електронної системи або серйозно заважають її роботі». Чи підпадає під дію цього закону «інформаційна операція» США в Іраку? Безперечно. Більш того, результатом цієї операції стало не лише порушення роботи іракської системи управління ППО, але й повне виведення її з ладу.

Розширення можливостей Інтернету і вступ суспільства в еру інформаційних технологій викликає появу нових видів злочинів та робить суспільство вразливим перед загрозою кібертероризму і злочинності.

Правоохоронці всього світу вважають своїм першочерговим завданням створення ефективної системи регулювання зростання злочинності в Інтернеті.

Безумовно, що глобальна інформаційна мережа Інтернет є важливим чинником прискорення світового прогресу, технологічною основою міжнародного інформаційного обміну. За цих умов інформаційні ресурси є величезною матеріальною цінністю, а несанкціонований доступ до цих ресурсів, якщо вони недостатньо захищені, може призвести до глобальних катастроф.

Тенденції злочинного використання досягнень у сфері телекомунікацій та інформатизації (збитки від кіберзлочинності, кібершахрайства та кібертероризму оцінюються в мільярди доларів) викликають необхідність вироблення єдиної міжнародної політики у сфері міжнародної інформаційної безпеки та створення міжнародного механізму контролю для попередження й припинення правопорушень у міжнародному інформаційному просторі.