УДК 343.3/7:004

КІБЕРТЕРОРИЗМ ТА ШЛЯХИ ЙОГО ПОДОЛАННЯ

І.В.Шаповалова,здобувач вищої освіти
Миколаївський національний аграрний університет

У статті проводиться огляд феномену кібертероризму, як глобальної проблеми. Розкриваються його особливості, можливі тенденції розвитку та методи захисту.

Ключові слова: *кібертероризм, інтернет ресурси, інформаційні технології, мережева та комп'ютерна безпека.*

Постановка проблеми. У сучасному світі з кожним днем інтернет все більше і більше вдосконалюється та збільшується у своїх масштабах. Створюється надзвичайно велика кількість сайтів для надання різного роду інформації, саме завдяки ним виникають нові можливості у комунікації та передачі знань на будь-яку відстань. У вільний час – сервіси надають різний медіа контент, в освіті – створюються нові електронні бібліотеки, в культурі – забезпечується перегляд витворів мистецтв та проведення виставок, тощо.

Проте цей процес не завжди несе в собі позитивні моменти. Надмірна доступність, слабкий контроль за даними і можливість обходу величезної кількості заборон роблять Інтернет вельми зручним інструментом для різних угруповань, що мають терористичний характер.

З кожним днем їх активність і вплив в мережі збільшується досить швидко, народжуючи нову глобальну проблему - кібертероризм. Через це багато держав і міжнародні організації, а зокрема ООН, приділяють велику увагу, видаючи різні укази і правові документи, що закликають до розробки заходів по боротьбі з нової світової загрозою.

Аналіз останніх новин і публікацій. Проблеми боротьби та розробки систем захисту інформації, окремі питання здійснення протидії комп'ютерній злочинності та інших факторів, стримуючих створення інформаційного суспільства, розглядались в роботах таких фахівців, як В.О. Голубєв, О.В. Возженніков, О. Гончарєнко, Є. Лисіцин та інших.

Над даною проблематикою також працювали такі вітчизняні та зарубіжні науковці різних соціальних сфер, як С. Хантінгтон, С. Хоффман, М. Делягін, В. Кутирьов, Г. Мірською, І. Міхеєв, В. Хорос, В. Антипенко,В. Крутов, В. Ліпкан, С. Телешун та інші [2].

Постановка завдання. Описати та відобразити важливість кібертероризму, як глобальної міжнародної проблеми, що вимагає активної розробки заходів для її вирішення.

Викладення основного матеріалу дослідження. Термін «кібертероризм» утворено злиттям двох понять: «кібер»(«кіберпростір») і «тероризм». ». У літературі все частіше зустрічаються терміни «віртуальний простір», «віртуальний світ». Беручи за основу поняття тероризму і поєднання його з віртуальним простором, можна вивести таке визначення: кібертероризм – це модель, яка виражається в навмисній, політично-

мотивованій атаці на інформацію, що оброблюється за допомогою комп'ютера і комп'ютерними системами,та створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України», кібертероризм – це терористична діяльність, що здійснюється у кіберпросторі або з його використанням [1].

Атаки з боку обчислювальних систем і мереж мають стихійний і непередбачуваний характер. Практично неможливо передбачити звідки і в якому вигляді буде виходити загроза, що зменшує шанси на її усунення. Основні труднощі даної проблеми полягають не в створенні і розборі комплексних систем дій спрямованих на її рішення, а в самому її визначенні. Це пов'язано з тим, що кібертероризм не постійний. Він не має чіткої і кінцевої форми, а багато його проявів мають суто індивідуальний характер.

Відмітна риса даного виду терору полягає в використанні різних програмних і апаратних засобів для реалізації своїх цілей. Вони можуть бути представлені як комп'ютерні віруси або троянські програми, здатні не тільки надати різну інформацію з віддалених мереж і машин, а і порушувати їх роботу. Так само це можуть бути спеціалізовані комп'ютерні обчислювальні станції, основна мета яких здійснювати кібератаки на різні інформаційні ресурси і сервіси, з подальшим виведенням їх з ладу.

Основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюються угрупованнями або окремими особами. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або придушувати кошти мережевого інформаційного обміну, здійснювати інші деструктивні дії. Ефективність же форм і методів кібертероризму залежить від особливостей інформаційної інфраструктури і ступеня її захищеності [3].

В основному, даний вид діяльності спрямований, на країни, інфраструктура яких безпосередньо пов'язана з комп'ютерними мережами. В першу чергу, її можна помітити по відношенню до державних або комерційних банківських систем, що завдає серйозний удар по фінансовим і економічним галузям. Другими в цьому списку є різні рекламні агентства і ЗМІ.

Проблема тут полягає в тому, що вони є всеохоплюючими інформаційними джерелами, які ніколи не були захищені від кібератак належним чином. Дана ситуація робить з них ідеальних посередників між терористами і їх жертвами, дозволяючи першим залишатися непоміченими, видаючи за себе різні станції телерадіомовлення або редакції газет, які розповсюджуються через мережу Інтернет.

Найчастіше кібертероризми здійснюються хакерами. Згідно з Оксфордським тлумачним словником, «хакер» - це особа, що намагається отримати несанкціонований доступ до комп’ютерних систем, зазвичай, з метою отримання секретної інформації [4].

Варто зазначити, що лише 0,1 % хакерів – це професіонали світового рівня, що становлять справжню загрозу, не тільки для якоїсь окремої компанії, а й для країни загалом. Незначний відсоток становлять хакери «середнього класу», які самостійно розробляють шкідливі програми та можуть становити загрозу для якоїсь компанії. Зазвичай кіберзлочинці такого класу об’єднуються у невеликі групи та разом атакують сайти. В окремих випадках їх наймають великі корпорації для заподіяння шкоди конкурентам. 90 % хакерів – це переважно підлітки, які мають базові навички програмування, та не представляють собою загрози для держави. Як правило, ці особи вчиняють злочини з метою задоволення почуття власної гідності. Вони шукають вразливі місця у програмному забезпеченні, намагаються обійти системи захисту сайтів

і, зазвичай, заробляють не багато, зламуючи акаунти в соціальних мережах та електронні поштові скриньки.

Комп'ютерні системи піддаються атакам хакерів кожного дня і це спричиняє неприємні наслідки для користувачів. Проте найбільшою проблемою є хакерські атаки на комп'ютери великих корпорацій та державних органів керування. Такі напади кіберзлочинців є загрозою, не лише функціональності якогось підприємства чи державного органу, а й економіки країни загалом.

У сукупності це дозволяє уявити, кібертероризм, як одну з задач, що вимагають швидкого і кардинального рішення. Особливість полягає в тому, що багато експертів в галузі мережевої та комп'ютерної безпеки, описують пошук методів для боротьби цією проблемою, як непередбачуваний в своєму протіканні процес. Вони говорять про те, що неможливо створити комп'ютерну обчислювальну систему, здатну повністю бути захищеною від різного роду злому або хакерських атак. Це пов'язано з тим, що яким би великим не був професіоналізм фахівця з безпеки комп'ютерних мереж, завжди є ймовірність що він не помітив маленький промах у захисті, який зможуть знайти зловмисники.

Ситуацію погіршує ще той факт, що багато кіберзлочинців не залишаються на одному і тому ж рівні своїх можливостей. Вони розвиваються, знаходять або розробляють нові способи злому, стають більш вправними і розумними, що ще сильніше ускладнює боротьбу з ними. Так само фахівці доповнюють, що можливо дана проблема буде актуальна ще довгий час, а точніше до тих пір, поки буде існувати простір для розвитку комп'ютерних технологій. Вони аргументують це тим, що кожна перемога кіберзлочинців, це теж маленький крок в розвитку обчислювальних систем, хоч несе в собі деструктивну функцію. Тому, єдиним кардинальним вирішенням цієї проблеми є, відмова від комп'ютерів і технологій, які вони нам подарували, але до такого кроку сучасне суспільство не готове.

Світові політичні лідери запропонували створити у Женеві (Швейцарії) Глобальний центр кібербезпеки, основною метою якого є побудувати безпечний і захищений глобальний кіберпростір. На думку політиків, кіберзлочинність неможливо подолати самотужки. Тому новий центр має створити першу міжнародну платформу для урядів, компаній, фахівців і правоохоронних органів для вирішення цієї проблеми. За словами експертів, щорічні втрати світової економіки унаслідок дій кіберзлочинців можуть досягати 500 мільярдів доларів.

Для порівняння, річний ВВП Швейцарії в 2017 році оцінюється в 659 мільярдів доларів. Всесвітній економічний форум у Давосі визнав, що кіберзлочинність є одним з найбільш критичних глобальних ризиків. У відповідь на них Глобальний центр кібербезпеки надаватиме підтримку урядам і галузевим компаніям, що є учасниками форуму, для створення безпечнішого кіберпростору з використанням підходу, що передбачає залучення численних зацікавлених сторін [5].

Загроза кібертероризму в даний час є дуже серйозною проблемою. Актуальність цього питання буде зростати в міру розвитку і поширення інформаційно-телекомунікаційних технологій. Вирішення проблеми кібертероризму є важливим при міжнародній інформаційній безпеці. Існують труднощі створення і збереження коаліцій при здійсненні міжнародного співробітництва. Так, з початком серйозного інформаційного акту тероризму міцність коаліцій держав піддається великому випробуванню, оскільки всі союзники поринуть в «інформаційний туман». Можуть виникнути і гострі проблеми з реалізацією спільних планів дій проти транснаціональної кримінальної або терористичної організації.

Висновок. Таким чином ситуація з тероризмом в мережах приймає особливе становище. Через її великий темп розвитку, все більше держав починають визнавати

його, як одну з найважливіших проблем сучасного світу, для ліквідації якої потрібно організувати ефективну співпрацю всіх країн. У зв'язку з цим, запобігання злочинам в цифровому середовищі і ліквідація їх наслідків мають дійсно глобальне значення.

Інфрмаційні джерела

1. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: закон України від 05.10.2017 № 2163-VIII; станом на 19.05.2018. – Електрон. текст. дані. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2163-19. – Дата останнього доступу : 05.10.2017. – Кібертероризм.

2. Топчій В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами [Електронний ресурс] / В. В. Топчій. – Електрон. текст. дані. – Режим доступу : http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf. – Дата останнього доступу : 19.05.2018. - Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами.

3. Ендрю Конрі- Мюррей Політика безпеки в часи терору [Електронний ресурс]. – Режим доступу : http://www.osp.ru/lan/2002/02/083.htm.

4. Оксфордський тлумачний словник англійської мови [Електронний ресурс]. – Режим доступу : http://www.oxforddictionaries.com/definition/english/hacker.

5. Світові лідери запропонували метод боротьби з кібертероризмом // Навчально-науковий центр інформаційних технологій [Електронний ресурс] / Електрон. текст. дані. – Режим доступу : http://nncit.tneu.edu.ua/svitovi-lideri-zaproponuvali-metod-borotbi-z-kiberterorizmom. – Дата останнього доступу :03.02.2018. - Світові лідери запропонували метод боротьби з кібертероризмом.

Науковий керівник - д-р екон. наук, доцент Клочан І. В.