

Ясенко О.\*

**БАЗИ ДАНИХ ЯК ОБ'ЄКТ КІБЕРТЕРОРИСТИЧНИХ АТАК**

*The article deals with the database hacking in the scope of cyberterrorism and introduces its own classification of cyberattacks on databases.*

*У даній статті йдеться про питання зламу баз даних у рамках поняття кібертероризму, а також представлена класифікація кібертерористичних атак на бази даних.*

Сучасні війни ведуться у першу чергу в інформаційному просторі. Те ж саме стосується і терористичних нападів, які становлять значну загрозу інформаційній безпеці будь-якої країни. Відсутність єдиного, затвердженого на наднаціональному рівні визначення кібертероризму та його видів створює певну понятійну плутанину, ускладнює роботу з фактичними даними, а тому потребує ретельного вивчення. На думку авторів, у межах поняття «кібертероризм» слід окремо виділити кібертерористичні атаки на бази даних.

Отже, метою даного дослідження є представлення класифікації кібертерористичних атак на бази даних за суб'єктами.

Дослідження ґрунтується на нижчезазначених дефініціях. По-перше, у Доповіді Дослідницької служби Конгресу зазначено: «Кібертероризм є окремим видом кіберзагроз, який відрізняється від інших (зокрема, кібервійни та кіберзлочинності) тим, що до числа його цілей можуть входити політична або економічна дестабілізація, саботаж, викрадення військових або громадянських активів та ресурсів у політичних цілях» [1]. По-друге, Закон України «Про авторське право і суміжні права» від 23 грудня 1993 р. визначає бази даних наступним чином: «Сукупність творів, даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі — електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп'ютера) чи інших засобів» [2].

Серед кіберзагроз, які виникають у сучасному світі, кібертероризм займає окреме місце — 12 % від усіх кібератак (за даними доповіді «The Web Hacking Incidents Database 2009») [3].

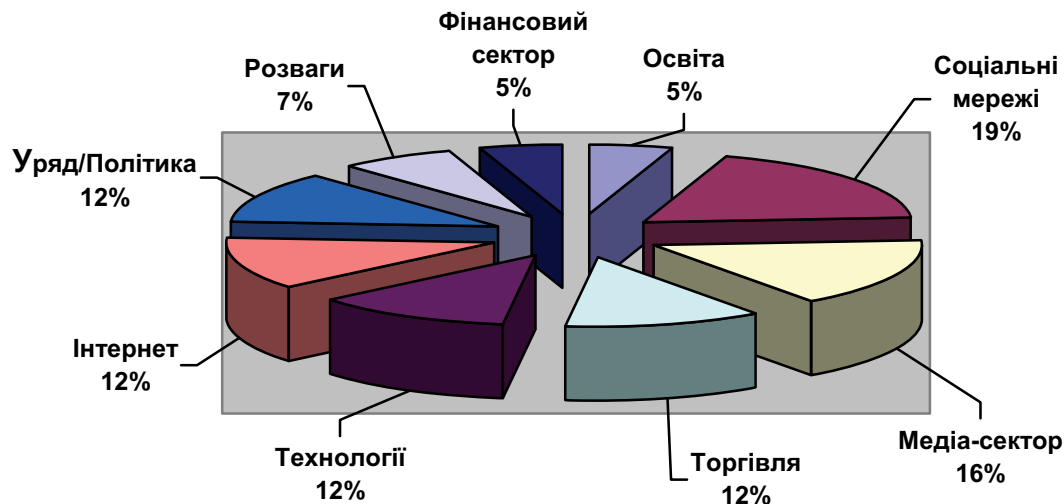
Пропонується класифікація, відповідно до якої кібертерористичні атаки на бази даних можна розділити на три категорії за суб'єктами:

- атаки з боку державних установ або на їх замовлення;
- атаки з боку певних організацій або на їх замовлення;
- атаки з боку фізичних осіб або на їх замовлення.

До першого типу кібератак можна віднести атаки китайських хакерів. Хакерський рух у Китаї організовано на державному рівні. Зокрема, Китай дозволив своїм кібертерористам об'єднатися в Honker Union of China (honker – гібрид англійського «hacker» і китайського «hong» — червоний) [4].

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

Науковий керівник: доц. Чичкань І.В.



Визначення прикладів на другий пункт видається проблематичним через те, що деякі організації можуть бути визнані терористичними лише в одній або декількох країнах. Тому для ілюстрації кібертерористичних атак на бази даних з боку терористичних організацій можна навести наступний приклад: у серпні 2010 р. прокуратура Туреччини завершила попереднє розслідування щодо заарештованих у березні 2010 р. двадцяти хакерів Робітничої партії Курдистану. Їх звинувачують у проникненні до бази даних соціальної мережі Facebook та вилученні звітних даних про 3800 державних посадовців та військових Туреччини [5].

Прикладом третього типу атак можна назвати випадок, коли німецький хакер Хесс Ландер зміг проникнути до бази даних Пентагону «ОРТ1М1». Зламавши її, він отримав доступ до 29 документів на тему ядерного озброєння, в тому числі, наприклад, до плану армії США у сфері захисту від ядерної, хімічної або бактеріологічної зброї [6].

Існують і більш неоднозначні ситуації. Так, наприклад, після захоплення «Флотилії свободи» у травні 2010 р. бази даних Ізраїлю були масовано атаковані хакерами — як правило, громадянами турецького походження. Таких осіб відносять до «тимчасових терористів». Попри назву, відповідно до представленої класифікації такі атаки відносяться до третього типу як атаки з боку фізичних осіб або на їх замовлення.

В нашому дослідженні представлена класифікація кібертерористичних атак на бази даних за суб'єктами. Тут викладаємо лише найбільш суттєві характеристики кожного з видів атак.

Розроблена класифікація кібертерористичних атак на бази даних дозволяє за наявності відповідної фактичної інформації визначити для кожної конкретної держави, на кого з суб'єктів припадає найбільша кількість скоєних атак. При аналізі кібертерористичної діяльності у світі або за окремими країнами слід враховувати, що при зміні, наприклад, показника атак з боку терористичних організацій зміняться пріоритетні напрями інформаційної безпекової політики держави.

### Література

1. Хилдрет С . Кібертероризм [Електронний ресурс] / С.Хилдрет. Режим доступу до ресурсу: <http://www.infousa.ru/information/bt-1028.htm>
2. Закон України «Про авторське право і суміжні права» від 23.12.1993 №3792-ХІІ [Електронний ресурс]. Режим доступу до ресурсу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3792-12>

3. The Web Hacking Incidents Database 2009 [Електронний ресурс]. Режим доступу до ресурсу: [http://www.breach.com/resources/whitepapers/downloads/WP\\_TheWebHackingIncidents-2009.pdf](http://www.breach.com/resources/whitepapers/downloads/WP_TheWebHackingIncidents-2009.pdf)
4. Міжнародна інформаційна безпека: сучасні виклики та загрози / [Макаренко Є.А., Рижков М.М., Ожеван М.А. та ін.] – К.: Центр вільної преси, 2006. – С.272-273
5. В Турції судят 20 курдських хакерів [Електронний ресурс]// *Новости Армении*. Режим доступу до ресурсу: <http://news.am/rus/news/28095.html>
6. Проблемы ядерного терроризма [Електронний ресурс]// Информационно-аналитическая служба СИП РИА. Режим доступу до ресурсу: [http://www.kuchaknig.ru/show\\_book.php?book=109234](http://www.kuchaknig.ru/show_book.php?book=109234)