О. Г. Корченко. Кібертероризм, комп'ютерний тероризм. *Енциклопедія Сучасної України* (2013)
ISBN 966-02-2074-X

О. Г. Корченко

Кібертероризм, комп'ютерний тероризм

КІБЕРТЕРОРИЗМ, Комп'ютерний тероризм К., який з'явився у 20 ст. разом з ін. новими формами *тероризму* – ядер., біол., хім., екол., психологічним, з огляду на масову інформатизацію суспільства, несе одну з найбільших загроз людству. Середовищем діяльності кібертерористів є кіберпростір – штучне електронне (віртуал.) середовище існування інформ. об'єктів у цифр. вигляді, утворене в результаті функціонування комп'ютер. систем упр. та оброблення інформації. Існує кілька визначень поняття «К.»: 1) застосування методів тероризму (створення в соц. сфері стану страху, неспокою, пригніченості з метою прямого або непрямого впливу на прийняття будь-яких рішень) у кіберпросторі; 2) навмисна, політично вмотивована атака на інформацію, яка обробляється комп'ютерами, комп'ютерну систему та мережі, що створює небезпеку для життя чи здоров'я людей або спричинює ін. тяжкі наслідки, якщо такі дії були вчинені з метою порушення громад. безпеки, залякування насел., провокації воєн. конфлікту тощо. 3) свідоме, цілеспрямов. застосування комп'ютер. інформації, комп'ютерів, комп'ютер. систем і мереж для захоплення комп'ютер. систем упр. потенційно небезпеч. об'єктами з метою: а) виведення цих об'єктів з ладу або їхнє руйнування, що прямо чи опосередковано створює або загрожує виникненням надзвичай. ситуації внаслідок цих дій і становить небезпеку для персоналу, насел. та довкілля; б) створення умов для аварій і катастроф техноген. характеру; в) залякування насел. та погрожування органам влади вчиненням вищезазначених протиправ. дій; г) вчинення провокацій воєн. конфлікту та міжнар. ускладнення; д) здійснення впливу на прийняття рішень, вчинення або невчинення дій органами держ. влади чи органами місц. самоврядування, служб. особами цих органів, об'єднаннями громадян, юрид. особами; забезпечення організац. чи ін. сприяння створенню або діяльності терорист. групи чи організації.

Загалом К. почав зароджуватися у 1970-х рр. 1983 заарешт. перших «віртуал. злочинців» – групу хакерів під назвою «банда 414» (м. Мілуокі, шт. Вісконсин, США), яка зламала 60 комп'ютерів (деякі з них належали Лос-Аламос. нац. лабораторії у шт. Нью-Мексико). Від поч. 1990-х рр. прояви К. з світ. резонансом відбуваються майже щорічно: 1993 у Лондоні

невідомі зловмисники погрожували атакою на комп'ютерну систему та мережі низці брокер. контор, банків і фірм та вимагали виплатити 10–12 млн фунтів стерлінгів відступних; 1995 група хакерів «Strano Network» здійснила потужну кібератаку на комп'ютери уряду Франції (перша атака типу «відмова в обслуговуванні», або DoS-атака); 1996 представники терорист. організації «Тигри звільнення Таміл-Ілама» провели мережеву атаку проти дипломат. представництв Шрі-Ланки; 1997 у результаті дій невстановленого хакера перервано передачу мед. даних між назем. станцією Нац. упр. з аеронавтики і дослідж. косм. простору США та косм. кораблем «Атлантіс»; 1998 12-річний хакер проникнув у комп'ютерну систему, що контролює паводк. шлюзи греблі ім. Т. Рузвельта в шт. Аризона (США), чим спричинив загрозу затоплення 2-х міст з насел. 1 млн осіб; 1999 в мережі Інтернет з'явився перший вірус під назвою «Хеппі-99» та відбулася широкомасштабна кампанія комп'ютер. атак Китаю та Тайваню один проти одного (постраждали портали держ. установ, фінанс. компаній, університетів тощо); 2000 із передмістя Маніли в мережу Інтернет запущено вірус «I love you» (ін. назва – «Love Bug»), що дуже швидко поширився світом і заразив понад 45 млн комп'ютер. мереж, зокрема й резиденції президента, Центр. розвідувал. упр., Міністерства оборони та Конгресу США, Британ. парламенту; 2001 шотланд. хакер Г. Маккінон зламав десятки комп'ютерів оборон. відомств, що стало найбільшою кібератакою на військ. комп'ютери в історії, та канад. 15-річний хакер Mafia Boy успішно реалізував DoS-атаку на декілька великих мережевих компаній (нанесена шкода оцінюється більш ніж у 1 млрд дол. США); 2004 здійснено масовану атаку на електронні ресурси уряду Пд. Кореї та 75 тис. спроб злому серверів Міністерства оборони США; 2005–06 зафіксовано більш ніж 2 млн кібератак на інформ. ресурси органів держ. влади в світі; 2007 відбулися масована атака на весь рос. інтернет-простір і потужна атака на сайти держ. структур Естонії; 2008 потужна кібератака на інформ.-комунікац. системи Грузії призвела до ізоляції груз. уряду та народу від зовн. світу; 2009 китай. спецслужбами проведено шпигун. кібероперацію «Ghostnet» з проникненням у комп'ютерні мережі більш ніж 100 країн світу; 2010 зафіксовано кібератаку перед самітом «Великої двадцятки» у Парижі, першу міжконтинентал. кібератаку «Стакснет» в Ірані, потужну DoS-атаку на інформ. інфраструктуру М'янми напередодні виборів; 2011 відбулися безпрецедент. витік даних у результаті кібератаки на сервери Міністерства оборони США, атака на сервери «Sony» та «Банк Америки» з подальшою публікацією конфіденц. інформації в мережі Інтернет, широкомасштабна кібератака перед самітом Євросоюзу в Брюсселі; 2012 хакер. група «Anonymous» пошкодила сайти Моссаду, армії та спецслужб Ізраїлю, у Швеції були реалізовані потужні кібератаки на Міністерство оборони, Упр. залізнич. доріг і «Шведбанк», зазнали вірус. атак електроенергет. компанії США, водночас амер. кіберексперти провели успішну атаку на пропагандист. сайт «Аль-Каїди» у Ємені. Низку кібератак зазнавали також сайти держ. установ України.

За даними «Лабораторії Касперського» на кін. 2012 найнебезпечнішими кіберзагрозами у світі є спеціально створена кіберзброя (програмні й апаратні засоби), маніпуляції у соц. мережах, онлайн-покоління (нове покоління, яке фактично живе у віртуал. світі і, як наслідок, дуже вразливе до кіберзагроз), втрата приватності (сучасні інформ. системи, форуми, портали та ін. змусили людство відмовитись від приват. життя і підсвідомо зробити його публічно доступним) та зламування мобіл. пристроїв (більшість людей щодня користується різними засобами комунікації: мобіл. телефонами, смартфонами, ноутбуками тощо, які є популяр. об'єктами посягань з боку кіберзлочинців і кібертерористів). 23 листопада 2001 Радою Європи прийнято Міжнар. конвенцію про кіберзлочинність (7 вересня 2005 ратифіковано ВР України). Цей документ був своєрід. реакцією на терорист. акти 11 вересня у США, його націлено на здійснення заг. політики з питань кримінал. права, метою якої є захист суспільства від К. шляхом прийняття потріб. законодав. актів, а також розширення міжнар. співробітництва. У Конвенції згадуються такі типи комп'ютер. злочинів: незакон. доступ; незаконне перехоплення; втручання в дані; втручання в систему; та засобів К.: комп'ютерна система, комп'ютерні дані, послуги інформ.-комунікац. технологій і дані трафіку. Також серед контрзаходів світ. спільноти варто виділити: 2009 – введення в США посади Нац. радника щодо кібербезпеки; 2011 – заснування у Великій Британії Міжнар. альянсу забезпечення кібербезпеки; 2009–12 – створення загонів кібервійськ у Китаї, США, Росії, початок формування аналогіч. укр. загонів, організація агентств кібернет. оборони у Австрії, Великій Британії, Німеччині, Швейцарії та Нідерландах, а також внесення вимог щодо забезпечення захисту від кіберзагроз у ключові нормативні документи критично важливих галузей нар. господарства (напр., цивіл. авіації). В Україні нині система підготовки кадрів у галузі інформаційної безпеки є досить розвиненою, чіткою та структурованою. Вона містить 3 напрями: «безпека інформ. і комунікац. систем», «системи тех. захисту інформації» та «упр. інформ. безпекою». Провідні ВНЗи з підготовки фахівців у галузі інформ. безпеки: Нац. авіац. університет, Нац. академія СБУ (обидва – Київ), Нац. тех. університет України «Київ. політех. інститут», Нац. університет «Львівська політехніка» та Харків. університет радіоелектроніки.

Рекомендована література

1. Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями. З., 2003;
2. Корченко О. Г. Системи захисту інформації. К., 2004;
3. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособ. Москва, 2004;
4. Компьютерная преступность и кибертерроризм. З., 2005. Вып. 3;
5. Конявский В. А., Лопаткин С. В. Компьютерная преступность: В 2 т. Москва, 2006;
6. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних: Підруч. К., 2009.

Бібліографічний опис:

Кібертероризм, комп'ютерний тероризм / О. Г. Корченко// Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. – К. : Інститут енциклопедичних досліджень НАН України, 2013. – Режим доступу: https://esu.com.ua/article-6747