Т Е М А V.

Кіберзлочинність та кібертероризм

План

1. Кіберзлочинність: поняття та сутність.
2. Поняття комп'ютерної злочинності. Загальна характеристика комп'ютерних злочинів.
3. Кібертероризм: поняття та сутність.

Пит. 1. Кіберзлочинність: поняття та сутність

Кіберзлочинність – це злочинність в так званому «віртуальному просторі». *Віртуальний простір (або кіберпростір)* – це модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді, що перебувають в процесі руху по локальних та глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки, передачі.

Виділяють такі ***ознаки кіберпростору***: 1) це інформаційний простір; 2) він є комунікативним середовищем; 3) утворюється за допомогою інформаційно-телекомунікаційних систем.

Кіберпростір можна розглядати як: 1) локальне середовище у разі функціонування засобу комп'ютерної техніки, який не підключено до мережі; 2) розосереджене середовище, яке виникає в разі підключення засобу комп'ютерної техніки до локальної або глобальної мережі передачі даних (Інтернету).[**]

На відміну від традиційних видів злочинів, історія яких налічує століття, кіберзлочинність – явище порівняно нове. Виділяють такі ***етапи розвитку кіберзлочинності:***

1 етап – поява кіберзлочинності та субкультури хакерів.

2 етап – розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності та національних груп хакерів.

3 етап – набуття кіберзлочинністю транснаціонального характеру, поява кібертероризму та міжнародних угруповань хакерів в усіх сферах кіберзлочинності.

4 етап – використання мережі Інтернет в політичних цілях, виникнення таких явищ, як Інтернет-страйк та Інтернет-війна, цілеспрямоване використання кібератак проти урядів окремих держав.[***]

Характерні властивості кіберзлочинності:

[**] Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності / О.В. Манжай // Право і безпека. – Харків : Вид-во Харківського національного ун-ту внутр. справ, 2009. – № 4 (31). – С. 215–219.

[***] Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності [Електронний ресурс] / В.Б. Дзюндзюк, Б.В. Дзюндзюк. – Режим доступу : http://nbuv.gov.ua.

1) *інтелектуальний характер* – здійснення кіберзлочину вимагає наявності спеціальних знань;

2) *анонімність і неперсоніфікованість* кіберзлочинів – механізми ідентифікації глобальної мережі дозволяють особі здійснювати операції анонімно або видавати себе за іншу особу, змінювати біографічні дані або соціальний статус;

3) *віддаленість* кіберзлочинів;

4) *висока латентність*;

5) *транснаціональність* – більше половини злочинів вчиняється у складі організованих груп, що знаходяться на території декількох країн;

6) *швидке зростання* кіберзлочинності, що пов'язане із дедалі більшим розповсюдженням та здешевленням Інтернет-послуг.*

Кіберзлочини – це суспільно небезпечні діяння, які пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами.

Найбільш поширена ***класифікація кіберзлочинів*** ґрунтується на *структурі Конвенції Ради Європи про кіберзлочинність.* У *першу групу* виділено злочини проти конфіденційності, цілісності та доступності комп`ютерних даних і систем, зокрема такі, як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. У *другу групу* входять злочини, пов`язані з використанням комп`ютера як засобу скоєння злочинів, а саме як засобу маніпуляцій з інформацією. У цю групу входять комп`ютерне шахрайство та комп`ютерне підроблення. *Третю групу* складають злочини, пов`язані з контентом (змістом даних, розміщених в комп`ютерних мережах). Найпоширенішим прикладом цих кіберзлочинів є злочини, пов`язані з дитячою порнографією. У *четверту групу* увійшли злочини, пов`язані з порушенням авторського права і суміжних прав. *П`ята група* злочинів зафіксована в окремому протоколі, зокрема це акти расизму та ксенофобії, вчинені за допомогою комп`ютерних мереж.

За об`єктом посягання* виділяються наступні групи кіберзлочинів: 1) злочини проти конфіденційності, цілісності та доступності комп`ютерних даних і комп`ютерних мереж; 2) економічні кіберзлочини; 3) кіберзлочини проти особистих прав і недоторканності приватної сфери; 4) кіберзлочини проти суспільних і державних інтересів. Водночас існує велика кількість кіберзлочинів, що зазіхають на декілька об'єктів.

Кіберзлочини також поділяють на:

• *традиційні злочини,* що вчиняються за допомогою комп'ютерних технологій та Інтернету, зокрема: порушення авторського права і суміжних прав (ст. 176 КК України); шахрайство (ст. 190 КК України); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх

---

* Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності [Електронний ресурс] / В.Б. Дзюндзюк, Б.В. Дзюндзюк. – Режим доступу : http://nbuv.gov.ua.

** Кіберзлочинність: проблеми боротьби і прогнози : наук. стаття [Електронний ресурс]. – Режим доступу : http://anticyber.com.ua/.

виготовлення (ст. 200 КК України); ухилення від сплати податків, зборів (обов'язкових платежів) (ст. 212 КК України); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України); незаконне збирання з метою використання або використання відомостей, що становлять комерційну чи банківську таємницю (ст. 231 КК України).

• *нові злочини,* що стали можливі завдяки новітнім комп'ютерним технологіям: несправжні Інтернет-аукціони; пошук та використання «проривів» (похибок) в програмах; розсилка листів (спам); азартні ігри в онлайн середовищі; викуп та реєстрація доменних імен (кіберсквоттинг); крадіжка послуг (фоункрейкинг); створення вірусів та інші.*

Способи протидії кіберзлочинності:

–побудова урядової моделі, спрямованої на забезпечення кібербезпеки;

–створення адекватного механізму протидії кіберзлочинності, заснованого на взаємодії приватного та державного секторів;

– чітке визначення прав та відповідальності приватного та державного сектора у сфері протидії кіберзлочинності;

–створення необхідної законодавчої бази;

–визначення ключових інформаційних інфраструктур, у тому числі основних активів, сервісів та взаємозалежностей;

–підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту ключових інформаційних інфраструктур;

–розробка системного та інтегрованого підходу до державного управління ризиками;

–підготовка вітчизняних фахівців у сфері кібербезпеки;

–посилення міжнародної співпраці.**

Пит. 2. Поняття комп'ютерної злочинності. Загальна характеристика комп'ютерних злочинів

Термін «кіберзлочинність» часто вживається поряд з терміном «комп`ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі, але не синонімічні. Поняття «кіберзлочинність» (в англомовному варіанті – cybercrime) ширше, ніж «комп`ютерна злочинність» (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі.

Так, Оксфордський тлумачний словник визначає префікс «cyber-» як компонент складного слова. Його значення – такий, що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Майже аналогічне визначення надає Кембриджський словник. Таким чином, «cybercrime» – це злочинність, пов`язана як з використанням комп`ютерів, так і

---

* Кіберзлочинність в Україні : наук. стаття [Електронний ресурс]. – Режим доступу : http://www.science-community.org/.

** Йона О.О., Казакова Н.Ф. Світові тенденції боротьби з кіберзлочинністю [Електронний ресурс] / О.О. Йона, Н.Ф. Казакова. – Режим доступу : http://dspace.oneu.edu.ua/.

з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» в основному відноситься до злочинів проти комп`ютерів або комп`ютерних даних.[***]

На думку Н.В. Савчук, поняття кіберзлочинності охоплює комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом вчинення злочину проти власності, авторських прав, громадської безпеки, моралі тощо. Отже, поняття «кіберзлочинність» та «комп'ютерна злочинність» співвідносяться як ціле та частина відповідно.[*]

Одним із засобів протидії кіберзлочинності є кримінально-правове забезпечення охорони суспільних відносин від визначених посягань шляхом закріплення правових норм, що встановлюють кримінальну відповідальність за такі злочини.

Чинний КК, а саме розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК містить шість статей:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361¹ КК);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361² КК);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363¹ КК).

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (комп'ютерні злочини) визначають як суспільно небезпечні та протиправні

[***] Скулиш Є.Д Теоретико-методологічні засади визначення об'єкта та предмета кіберзлочинів / Є.Д. Скулиш // Правова інформатика. – № 2 (42). – 2014. – С. 48.

[*] Голубєв В. Кібертероризм – загроза національній безпеці та інтересам України [Електронний ресурс] / В. Голубєв. – Режим доступу : http://www.justinian.com.ua/.

діяння, що посягають на суспільні відносини у сфері безпеки комп'ютерної інформації та нормального функціонування електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку, заподіюючи їм шкоду чи ставлячи під загрозу заподіяння такої шкоди.[**]

Пит. 3. Кібертероризм: поняття та сутність

Із появою кібертероризму кіберзлочинність набула ознаки транснаціональності, його поява ознаменувала початок третього етапу розвитку кіберзлочинності.

Під *комп'ютерним тероризмом (кібертероризмом)* слід розуміти умисну, політично вмотивовану атаку на інформацію, яка обробляється комп'ютером, комп'ютерну систему і мережі, що створює небезпеку для життя і здоров'я людей або настання інших тяжких наслідків, якщо такі дії були скоєні з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту.[*]

Цілі здійснення кібертероризму збігаються з цілями і мотивами здійснення всіх відомих видів терористичних дій, а саме: порушення суспільної і державної безпеки; залякування населення; провокація військового конфлікту; ускладнення міжнародних відносин; вплив на прийняття рішень або здійснення (нездійснення) дій органами державної влади та місцевого самоврядування, посадовими особами цих органів, об'єднаннями громадян, юридичними особами; привертання уваги громадськості до певних політичних, релігійних та інших поглядів.

Комп'ютерний тероризм (кібертероризм) передбачає інформаційні атаки на обчислювальні центри, центри управління воєнними мережами й медичними закладами, банківські та інші фінансові мережі, засоби передачі даних за допомогою комп'ютерних мереж. Він може здійснюватися *з метою* саботажу (урядових установ), заподіяння економічного збитку (великим виробничим корпораціям), дезорганізації праці з потенційною можливістю смертей. Інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюється терористичними угрупованнями або окремими особами, є основною *формою* кібертероризму. Така атака дозволяє проникати у систему, перехоплювати управління або пригнічувати засоби інформаційного обміну в мережі, чинити інші деструктивні впливи.[**]

Засоби здійснення можуть бути різноманітними і включати всі види сучасної інформаційної зброї. Поряд із такими засобами ураження

[**] Кузнецов В.В. Кримінальне право України : посібник [Електронний ресурс] / В.В. Кузнецов. – Режим доступу : http://westudents.com.ua/.

[*] Голубєв В. Кібертероризм – загроза національній безпеці та інтересам України [Електронний ресурс] / В. Голубєв. – Режим доступу : http://www.justinian.com.ua/.

[**] Бутузов В.М., Тітуніна К.В. Сучасні загрози: комп'ютерний тероризм : наук. стаття [Електронний ресурс] / В.М. Бутузов, К.В. Тітуніна. – Режим доступу : http://www.irbis-nbuv.gov.ua.

інформаційних комп'ютерних систем, як комп'ютерні віруси, програмні пристрої, слід зазначити засоби пригнічення інформаційного обміну в телекомунікаційних мережах, його фальсифікації та засоби, що дозволяють впроваджувати програмні закладки у державні та корпоративні інформаційні системи й управляти ними на відстані. До таких засобів належить, наприклад, нейтралізатор тестових програм, що забезпечує неможливість виявлення природних і штучних недоліків програмних засобів спеціальними тестовими програмами.

Тактика і прийоми, що використовуються при вчиненні цього злочину, відрізняються від тактики і прийомів вчинення класичних комп'ютерних злочинів тим, що комп'ютерний терористичний акт повинен мати небезпечні наслідки, стати широко відомим населенню й одержати великий суспільний резонанс.

Від комп'ютерних злочинів кібертероризм відрізняється насамперед своїми цілями, що властиві тероризму в цілому: дії завжди мають публічний характер і спрямовані на вплив, що здійснюється відносно окремих осіб, суспільства чи влади. Від традиційного тероризму (політики залякуванням, пригнічення супротивників здійсненням актів насильства) він відрізняється засобами здійснення, а також своєю анонімністю та знеособленістю.

Розглядаючи структуру та сутність кібертероризму як інформаційного протиборства, до його основних ***напрямів*** слід віднести:

1) здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів подолання систем захисту інформаційних і телекомунікаційних систем супротивника), що призводить до витоку, втрати, підробки, блокування інформації або до порушення встановленого порядку її маршрутизації;

2) створення та використання шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

3) здобуття необхідної інформації шляхом несанкціонованого втручання в інформаційні потоки, що передаються каналами зв'язку, чи бази даних, що перебувають в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку;

4) пригнічення елементів інформаційної інфраструктури державного або приватного сектору економіки.[*]

Пропонується виділяти такі ***напрями боротьби з кібертероризмом:***

— уніфікація та гармонізація національного законодавства та міжнародних актів;

— розробка єдиного понятійного апарату;

— удосконалення критеріальної основи безпеки інформаційних систем;

[*] Бутузов В.М., Тітуніна К.В. Сучасні загрози: комп'ютерний тероризм : наук. стаття [Електронний ресурс] / В.М. Бутузов, К.В. Тітуніна. – Режим доступу : http://www.irbis-nbuv.gov.ua.

— проведення наукових досліджень у сфері створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

— створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом із ефективною системою координації їх взаємодії;

— удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

— удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки.[*]

[*] Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії : наук. стаття [Електронний ресурс] / С.Б. Гавриш. – Режим доступу : http://www.irbis-nbuv.gov.ua.