Презентація на тему: Кіберзлочинність

Виконав:

Хнипель Євген

Поняття кіберзлочинності

- Кіберзлочинність - це злочинність у так званому кіберпросторі. Автори «модельного закону» про кіберзлочинність Міжнародного Союзу Електрозв`язку (2009 р.) визначають кіберпростір як « фізичний і не фізичний простір, створений і (або) сформований таким чином: комп`ютери, комп`ютерні системи, мережі, їхні комп`ютерні програми, комп`ютерні дані, дані контенту, рух даних, і користувачі». В даний час офіційне визначення кіберпростору на міжнародному рівні відсутнє, втім, як і визначення кіберзлочинності.

- Термін «кіберзлочинність» часто вживається поряд з терміном «комп`ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, але все-таки, на наш погляд, 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 приставку «cyber - » як компонент складного слова. Її значення - що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник. Таким чином, «cybercrime» - це злочинність, пов`язана як з використанням комп`ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» в основному відноситься до злочинів, скоюваних проти комп`ютерів або комп`ютерних даних.

СОЦИАЛЬНОЕ ХАКЕРСТВО

Существуют обходные пути к ценной информации. Так, хакеры целенаправленно заражают недостаточно защищенные ПК сотрудников, чтобы заполучить данные доступа к системам безопасности компаний. После этого часто уже не представляет труда проникнуть на сервер фирмы.

ЛОВУШКИ В СОЦИАЛЬНЫХ СЕТЯХ

Через социальные сети на незащищенных компьютерах вредоносный код распространяется еще быстрее.

ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ
УЯЗВИМОЕ СОЕДИНЕНИЕ

- У 2013 р. Управління ООН з наркотиків і злочинності в опублікованому звіті «Всебічне дослідження проблеми кіберзлочинності та відповідь заходів з боку держав - членів, міжнародного співтовариства і приватного сектора» відзначає, що поняття «кіберзлочинність» залежить від контексту і мети вживання цього терміна. При цьому, як наголошується в тому ж документі, що хоча основне "ядро" цього терміна представляють злочини проти конфіденційності, цілісності та доступності даних, крім цього досить обмеженого списку комп`ютерних злочинів, в поняття «кіберзлочинність» включаються будь-які дії, спрямовані на нелегальне вилучення прибутку, контент-злочини, та інші протизаконні діяння в кіберпросторі. При цьому, як відзначають автори звіту, у створенні якогось універсального визначення кіберзлочинності немає необхідності, так як, наприклад, з метою міжнародного співробітництва в розслідуванні злочинів набагато важливіше гармонізувати норми, що відносяться до збору та поданням електронних доказів. Ця необхідність не обмежується якимось штучним терміном «кіберзлочинів», оскільки на електронних носіях і в електронних комунікаціях може міститися інформація, що відноситься до будь-якого виду злочинів, скоєних як у кіберпросторі, так і поза ним.

Види кіберзлочинів

- Кіберзлочини поділяють на види залежно від об`єкта, від предмета посягання, залежно від способів скоєння і т. п.

- По об`єкту посягання виділяються наступні групи кіберзлочинів: злочини проти конфіденційності, цілісності та доступності комп`ютерних даних і комп`ютерних мереж, економічні комп`ютерні злочини, комп`ютерні злочини проти особистих прав і недоторканності приватної сфери, комп`ютерні злочини проти суспільних і державних інтересів. Проте варто відзначити, що багато кіберзлочинів зазіхають відразу на декілька об`єктів: наприклад, незаконне перехоплення приватних електронних комунікацій зазіхає на недоторканність приватної сфери і на конфіденційність комп`ютерних даних, комп`ютерне шахрайство - на власність і на цілісність комп`ютерних даних і т.д.

Найбільш поширена класифікація кіберзлочинів в даний час грунтується на структурі Конвенції Ради Європи про кіберзлочинність спочатку підрозділяється кіберзлочини на чотири групи (потім був прийнятий додатковий протокол, і тепер груп - п`ять). Ця класифікація в даний час є «еталоном», оскільки наявні міжнародні та регіональні документи, а також наукова практика, слід саме цьому підрозділу комп`ютерних злочинів на п`ять груп.

- У першу групу виділено злочини проти конфіденційності, цілісності та доступності комп`ютерних даних і систем, 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 засіб маніпуляцій з інформацією. У цю групу входять комп`ютерне шахрайство та комп`ютерне підроблення.

- Третю групу складають злочини, пов`язані з контентом (змістом даних). У цю групу входять злочини, пов`язані з контентом - тобто з вмістом даних, розміщених в комп`ютерних мережах. Найпоширеніший і караних практично у всіх державах вигляд цих кіберзлочинів - злочини, пов`язані з дитячою порнографією.

- У четверту групу увійшли злочини, пов`язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав.

П`ята група злочинів зафіксована в окремому протоколі - це акти расизму та ксенофобії, вчинені за допомогою комп`ютерних мереж.

Стан, структура і динаміка кіберзлочинності

- Кіберзлочинність - явище за своєю природою транскордонне. Тому аналіз кіберзлочинності або його різновиду - комп`ютерної злочинності - у рамках однієї країни чи групи країн, безумовно, цінний, але навряд чи здатний дати уявлення про справжні масштаби і про розмах цього явища. Глобальність і транскордонність комп`ютерних і телекомунікаційних мереж, можливість маніпуляцій злочинця з ідентичністю (тобто використання чужих імен, адрес, паролів і т.п.) створює ситуації, коли злочинець знаходиться на одному континенті, злочин безпосередньо вчиняється на іншому, а наслідки злочину наступають на третьому. Більше того, в останні кілька років у зв`язку з появою і поширенням ботнетів - мереж інфікованих комп`ютерів, які проводять атаки незалежно від користувачів, ситуація ускладнилася ще більше: злочинець, сотні атакуючих комп`ютерів і потерпілий від злочину можуть перебувати на території більш ніж двох або трьох держав.


INTERPOL

- Для більшості злочинів, скоєних в глобальних комп`ютерних мережах, характерні наступні особливості: підвищена скритність вчинення злочину, що забезпечується специфікою мережевого інформаційного простору (розвинені механізми анонімності, складність інфраструктури тощо); транскордонний характер мережевих злочинів, при якому злочинець, об`єкт злочинного посягання, потерпілий можуть перебувати на територіях різних держав; особлива підготовленість злочинців, інтелектуальний характер злочинної діяльності; нестандартність, складність, різноманіття і часте оновлення способів скоєння злочинів і застосовуваних спеціальних засобів; можливість вчинення злочину в автоматизованому режимі в декількох місцях одночасно, можливість об`єднувати відносно слабкі ресурси багатьох окремих комп`ютерів в потужне знаряддя вчинення злочину; багатоепізодним характер злочинних дій при множинності потерпілих; необізнаність потерпілих про те, що вони піддалися злочинному впливу; дистанційний характер злочинних дій в умовах відсутності фізичного контакту злочинця і потерпілого; неможливість запобігання та припинення злочинів даного виду традиційними засобами.

Проблеми боротьби з кіберзлочинністю

- Відсутність механізмів контролю. Основна проблема боротьби зі злочинністю в мережі Інтернет полягає в транснаціональності самої мережі і у відсутності механізмів контролю, необхідних для правозастосування. Коли мережа Інтернет створювалася технологічно як структура без ієрархії і без якогось «ядра», зруйнувавши які, можна було б паралізувати її роботу, навряд чи хтось міг уявити масштаби розвитку проекту, спочатку не призначеного для широкої аудиторії. Основною метою створення цієї мережі була стійкість до атак ззовні, і навряд чи хтось міг передбачити подальший масштаб її розвитку та її соціальну та економічну роль у майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини укупі з її доступністю і легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі і відсутність національних кордонів у кіберпросторі зумовили можливості для зростання злочинності та на роки відклали розробку механізмів соціального та правового контролю у сфері використання інформаційних мереж для вчинення злочинів.

Боротьба з Кіберзлочинністю

- Базовим міжнародним нормативно-правовим документом, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю, є Конвенція Ради Європи "Про кіберзлочинність" від 23 листопада 2001 року.
- Європейський Союз лише готується до імплементації Конвенції. Першими кроками на цьому шляху були Спільна Позиція 1999/364/Л НА від 27 травня 1999 року, затверджена Радою ЄС на підставі ст. 34 Договору про заснування ЄС щодо переговорів відносно проекту Конвенції про комп'ютерну злочинність, які відбулися у Раді Європи, та Пропозиції для Рамкового Рішення Ради ЄС щодо атак, спрямованих на інформаційні системи.
- Цікавим є той факт, що, аналізуючи нормативно-правові акти ряду країн Європейського союзу, відповідно до яких закріплена відповідальність за передбачені даною Конвенцією діяння, найбільше відповідає конвенціальним нормам Кримінальний кодекс Німеччини.

На цьому презентація закінчена
Дякую за увагу!!