УДК 004.056

Заворуєв Р.С., Резніченко В.А.
Кіровоградський національний технічний університет

Протидія кіберзлочинності в Україні

Кіберзлочинність є явищем новітньої, цифрової доби. Саме це й робить «кіберів» набагато небезпечнішими й ефективнішими за своїх «класичних» колег - шахраїв. Це люди, які працюють головою і роблять свої «справи», не відходячи від свого комп'ютера або сидячи на лавочці з ноутбуком і мобільним телефоном. Для сучасних «технарів» це часто ідеальний спосіб заробити і реалізувати себе. Злочинці не стоять на місці. Їхні методи вдосконалюються і стають дедалі складнішими. Відповідно, реагують і правоохоронці. Останнім часом рівень кіберзлочинності швидко зростає в Україні. Експерти зазначають, що Україна - дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм та меншою мірою - Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування.

СБУ і МВС в особі Управління боротьби з кіберзлочинністю опинилися на вістрі війни з «кіберами». Нажаль, їхніх зусиль замало. Особливо, зважаючи на наші українські реалії. Якщо раніше українські програмісти- хакери писали вчинені віруси для злому і розкрадання даних в багатих західних країнах, то тепер у зв'язку з посиленням боротьби американської і європейської влади з комп'ютерними злочинами їхня увага звернулася і на Україну.

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем -це далеко не повний перелік інтернет злочинів. Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, високим збитком навіть від одиничного злочину.

Кіберзлочини можна класифікувати на два види:традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету та нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям.

За оцінками експертів, в останні місяці в управлінні з боротьби з кіберзлочинністю тільки в Києві фіксується до двадцяти випадків крадіжки грошей через клієнт-банк. Суми становлять від 20 тис. до 40 млн. грн. Однак подібні факти замовчуються, повідомлень в ЗМІ про них практично немає. Ні потерпілим, ні банкам, ні міліції не вигідний галас

навколотого, що відбувається. У ряді випадків бувають ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків та силових структур.

Українською проблемою є як недостатня кількість державних експертів в області комп'ютерно-технічної експертизи, так і складнощі з введенням в правове поле досліджень фахівців комерційних організацій. Типовий термін проведення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ. Весь цей час підозрюваний може перебувати в СІЗО. На все це накладається набуття чинності 19 листопада 2012 року нового КПК, який встановлює нові і поки «незрозумілі» правила взаємодії всіх учасників процесу. У зв'язку з посиленням європейського законодавства кіберзлочинці можуть перекочувати в менш захищену Україну.

Українське ж законодавство у сфері захисту інформації, на думку Ю.Омельченка, вимагає дуже серйозного доопрацювання. «Потенційно існує ймовірність того, що кіберзлочинність буде виштовхуватися з Європи, то вона буде перебиратися в Україну. Та й уже цей процес відбувається», -зазначив експерт.

При цьому директор департаменту Microsoft відзначив, що іноземці дуже високо цінують українські «світлі голови» і щосили вже використовують їх знання для вчинення протиправних дій. У зв'язку з цим представник СБУ Тарас Бєлов нагадав, що минулого року правоохоронні органи «розібралися» з цілою групою таких осіб, які продавали свої -дуже висококласні -хакерські розробки за кордон.

Таким чином, кіберзлочинність - це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи вміст кишень пересічних громадян. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців. Але аналіз сучасного громадського життя показує, що найекзотичніші та малочисельні в недалекому минулому для нашого суспільства злочини зараз отримують дуже широке розповсюдження та серйозний суспільний резонанс.

Список використаних джерел

1. *Острейковскій В.А. Інформатика: Учеб. посібник для студ. середовищ. проф. навч. закладів. - М.: Вищ. шк., 2001. - 319с.*
2. *Економічна інформатика / під ред. П.В. Конюховского і Д.М. Колесова. - СПб.: Пітер, 2000. – 560 с.*
3. *Інформатика: Базовий курс / С.В. Симонович та ін - СПб.: Пітер, 2002. - 640с.*
4. *Молдовян А.А., Молдовян Н.А., Рад Б.Я. Криптографія. - СПб.: Видавництво "Лань", 2001. – 224 с.*