Проблеми попередження організованої кіберзлочинності

Воробей В.М., студент ННІПП НАВС
Науковий керівник: кандидат юридичних наук, доцент *Раєцька Л.В.*

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

Кіберзлочинність - це злочинність у так званому »віртуальному просторі».Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера інформаційний, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі. [1,с.32]

Першою причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова, а це означає що профілактичними заходами в даному випадку можуть бути дії спрямовані на регулярну перевірку рахунків тих, хто потрапляв хоч один раз в поле зору з даних питань.

Друга причина росту кіберзлочинності як бізнесу - те, що успіх справи не пов'язаний з великим ризиком.

Кіберзлочинність – явище новітньої, цифрової доби. Саме це й робить «кіберів» набагато небезпечнішими й ефективнішими за своїх «класичних» колег-шахраїв. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній. За деякими оцінками, через кіберзлочинців щорічно світова економіка втрачає $ 114 млрд, повідомляє РБК. А США оцінили свої збитки за всі роки існування глобальної мережі у $ 400 млрд. Це у три рази більше щорічних витрат на освіту. Варто працювати над створенням профілактичних напрямів роботи, розробляти концепції, програми плани дії.

Превентивні заходи вже не допомагають, і з кожним роком шкода збільшується, а злочини стають все більш «вишуканими». Найпоширеніші - це злом баз даних компаній та урядових організацій, виведення з ладу промислових об'єктів. До цього, наприклад, призвела атака вірусу на іранську АЕС у Бушері. Також широко відомі крадіжки інновацій або технологій і, нарешті, банальна крадіжка грошей.

Україна увійшла до трійки лідерів з DDoS-атак. За даними Лабораторії Касперського, 12% від усіх атак припадає на Україну.

Так, 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. У ряді випадків бувають ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків та силових структур.[2,с.9].

Зовсім не так давно, національне агентство з боротьби зі злочинністю

великої Британії, британський аналог ФБР заарештувало 23-річного підозрюваного у скоєнні кібератаки на міністерство оборони США 15 червня 2014 року від імені хакерського угруповання Lizard Squad.

Тоді в результаті атаки стався витік даних 800 співробітників Пентагону, включаючи їх імена, посади, адреси електронної пошти та номери телефонів. В результаті злому системи Пентагону були оприлюднені дані міжнародної супутникової системи розповсюдження повідомлень (EMSS).

Як заявили в NCA, серед злочинів, які ймовірно вчинили затримані в період з 2 по 6 березня, такі види кібератак, як злом та крадіжка даних транснаціональних компаній і держустанов, DdoS-атаки, кібершахрайство, поширення вірусів і шкідливого ПЗ [3].

Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм.

Список використаних джерел:

1. Біленчук Д.П. Кібрешахраї – хто вони? //Міліція України, 1999. №7-8. С.32-34
2.Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. - //Економічна правда від 26 лютого, 2013року.
3. КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ [Електронний ресурс]. – Режим доступу: http://www.science-community.org/ru /node/16132

Маргінальність та злочинність

Геращенко В.І., студент ННІПП НАВС
Науковий керівник: кандидат юридичних наук, доцент *Раєцька Л.В.*

Феномен маргінальності відноситься до характеристики стану особистості, яка піддається певним випробуванням, викликаним переходом індивідів з однієї соціокультурної середи в іншу. Найбільш вираженим випадком такого переходу є спадна соціальна мобільність і вимушена міграція індивідів. У підсумку виходить, що мова йде про характеристики свідомості, поведінки та способу життя особистості, що опинилася на межі різних культур, соціальних груп, спільнот (культурна маргінальність, маргінальність соціальної ролі, структурна маргінальність).

У 80-і роки для радянських кримінологів саме цей аспект залишався єдиним і головним у розумінні маргінальної середовища: це – соціально нестійка декласована і полудеклассірованная соціальна група, як правило, включає нероб, волоцюг, алкоголіків, наркоманів, соціально неадаптованих суб'єктів з кримінальним минулим, які значно ускладнюють кримінологічну обстановку [1].

Взаємозв'язок маргінальності та злочинності в даному випадку може трактуватися не тільки у вигляді припущення, що маргінал в силу