Марков Михайло Миколайович,
професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, доцент

КІБЕРЗЛОЧИННІСТЬ Й ЕКОНОМІКА

Якщо розглянути економічну злочинність, то вона не має меж. Адже має вплив на різні організації по всьому світі і жодна галузь економіки або компанія не може відчувати себе повністю захищеною від небажаних наслідків економічної злочинності.

Всесвітній огляд економічних злочинів робить акцент саме на зростаючу загрозу кіберзлочинності. У наш час багато людей і організацій використовують різні інноваційні технології, включаючи Інтернет. Таким чином, вони є схильними до ризику потенційних атак шахраїв з будь-якого куточка світу. На тлі проблем розкрадання даних і витоку інформації, комп'ютерних вірусів і атак хакерів, особливу увагу потрібно приділити значущості цього виду економічної злочинності та його впливу на організації в усьому світі.

Кіберзлочинність знаходиться на п'ятій сходинці за значимістю економічної злочинності в Україні, слідом за незаконним привласненням майна, хабарництвом і корупцією, практикою підриву конкуренції і маніпуляцією з фінансової звітністю.

Згідно результатів опитування спеціалістами PwC, то на кіберзлочинність припадає 23% випадків шахрайства в світі, про які повідомили учасники опитування, і 17% в Україні. Дані огляду в сфері інформаційної безпеки свідчать про те, що кіберзлочини стають більш витонченими, що ускладнює їх виявлення та запобігання. Це може привести до ще більших збитків і втрат в майбутньому [1].

Є такі причини розповсюдження кіберзлочинності:

- саме ця сфера злочинної діяльності є дуже прибутковою та стає в один ряд з такими незаконними сферами діяльності, як незаконний обіг наркотиків, зброї та торгівля людьми;
- фінансові установи приховують від правоохоронних органів більшість фактів кібератак на свої установи, піклуючись про свою репутацію серед клієнтів;
- за умови незначних фінансових втрат, фінансові установи не проводять навіть внутрішніх розслідувань з огляду на те, що людські, фінансові та інші затрати на таке їх проведення значно перевищують втрати;
- злочини вчиняються у віртуальному середовищі, тобто є дуже латентними.

Існує багато видів кримінальних правопорушень, пов'язаних із використанням комп'ютерів в економіці [2], у рамках яких має місце

розкрадання грошових коштів: атаки хакерів на банки або фінансові системи; шахрайства, пов'язані з переказом «електронних» грошей; шахрайства з банківськими пластиковими картами та ін.

Існує багато видів економічних злочинів, причому деякі з них є більш поширеними і зустрічаються набагато частіше від інших. Повертаючись до опитування спеціалістів PwC, то найбільш поширеним видом економічних злочинів в Україні виявилось незаконне привласнення майна (73%), на другому місці опинилося хабарництво і корупція (60%), на третьому – маніпуляції з фінансовою звітністю (30%) [1].

Результати опитування свідчать про те, що українські компанії набагато більше страждають від «Хабарництва і корупції» та «Практики недобросовісної конкуренції», ніж інші країни в Центральній і Східній Європі та світі.

На сьогодні кіберзлочинність – це реальна глобальна загроза, яка може виходити з будь-якої країни світу, а також за рамки конкретної юрисдикції на відміну від багатьох інших традиційних видів економічних злочинів. Для ефективної боротьби з кіберзлочинністю потрібна система заходів і реалізація відповідної державної політики в цій галузі. Одні лише нові закони не здатні протистояти зростанню IT-злочинності. Потрібен комплекс заходів, спрямованих не лише на розвиток правозастосовної бази, але й на підвищення рівня грамотності громадян, судових та правоохоронних органів [3].

Одне з головних завдань – це організація плідної взаємодії з правоохоронними органами у сфері боротьби з кіберзлочинністю, а також надання допомоги компаніям, що постраждали від кібератак [4].

Список використаних джерел

1. URL: https://www.pwc.com/ua/ru/press-room/assets/gecs_ukraine_ru.pdf.

2. Geer D. Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. Geer Risk Services, LLC. URL : http://www.verdasys.com/mt_geer.php.

3. ФБР расследует взлом твиттера Associated Press. Материалы ресурса lenta.ru. URL : http://lenta.ru/news/2013/04/24/investigation.

4. Kavun S. (2013). Management of corporate security: new approaches and future challenges. Editorial Denis Galeta and Miran Vrsec. Cyber security challenges for critical infrastructure protection (pp. 141–151) / S. Kavun, R. Brumnik. Ljubljana : Institute for Corporate Security Studies. Retrieved August 5, 2013, from http://www.ics-institut.com/research/books/5.