УДК 351.863:339.9

О. І. Вівчар, канд. екон. наук, доц., член кореспондент Академії економічних наук України

Тернопільський національний економічний університет

ПРОБЛЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ У СОЦІОГУМАНІТАРНІЙ СФЕРІ

O.I. Vivchar, Ph. D., Assoc. Prof.

PROBLEMS OF ECONOMIC SECURITY IN SOCIAL SPHERE

В умовах гібридної війни, тотального використання засобів масової інформації та її комунікаційних складових особливої актуальності набуває попередження основних загроз кіберзлочинності. Результати наукових досліджень проблематики кіберзлочинності непокоїть не тільки державу в цілому, а й кожного окремо взятого господарюючого суб'єкта, від малого до великого.

Кіберзлочинність – використання комп'ютера як інструмента нелегальних дій, таких як шахрайство, торгівля інтелектуальною власністю, крадіжка особистих даних та інших складових, що порушує недоторканність різних сфер функціонування.

Хотілося б зазначити, що найбільш поширеними видами злочинів, пов'язаних із використанням інформаційних технологій підприємницьких структур країни, є: злочини у сфері комп'ютерних та Інтернет-технологій – 26 %, злочини у сфері функціонування електронних платежів чи платіжних карток – 16 %, злочини у сфері телекомунікацій – 11 %, злочини у сфері використання комп'ютерних технологій при скоєнні традиційних злочинів – 47 %. Звертаємо увагу на те, що такі злочини характеризуються високим рівнем технічного забезпечення, латентністю, організованістю, наявністю міжрегіональних та міжнародних зв'язків [2].

Неможливо залишити поза увагою те, що сучасна соціогуманітарна субкультура хакерів має кримінальну основу, оскільки її можна визначити як сукупність ідей, цінностей, звичаїв, традицій, норм поведінки, направлених на організацію способу життя, метою якого є вчинення комп'ютерних злочинів, їх приховування і ухилення від відповідальності.

Слід зазначити, що в умовах проникнення кіберзлочинності в соціогуманітарну сферу підприємницького і державного життя, її подолання, стає основоположним чинником на шляху входження України в світовий інформаційний простір. Одразу ж зауважимо, що кіберзлочинність – неминучий наслідок глобалізації інформаційних процесів і як наслідок є основною загрозою соціогуманітарної компоненти підприємств.

Для комплексної протидії кіберзлочинності на підприємствах пропонується: гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні; розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонної проблематики; налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні; механізм вирішення юрисдикційних питань у кіберпросторі [1].

Резюмуючи зазначимо, що кіберзлочинність як основна загроза економічній безпеці підприємств потребує невідкладних науково-практичних розробок в царині науки та посилення навчальної компоненти. Звертаємо увагу на те, що керівники підприємницьких структур повинні знати не лише про масштаби нанесення шкоди, а можливі наслідки даної злочинної діяльності.

Література:

1. Vivchar O. Peculiarities of assessment technologies usage in the management of financial and economic security of enterprises / O. Vivchar // Business Economics – Issue 4 (2), (October). Volume 51. "Palgrave Macmillan Ltd.", 2016. – Pages 393-398.

2. McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Електронний ресурс] // An Intel Company. – Режим доступу \www/ URL: http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx.