УДК 343.3+316.334.3

Оксана Вівчар
Тернопільський національний економічний університет

СОЦІОГУМАНІТАРНИЙ ВИМІР: КІБЕРЗЛОЧИННІСТЬ ЯК ОСНОВНА ЗАГРОЗА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Oksana Vivchar

MODERN SOCIAL DIMENSION: CYBERCRIME AS A MAJOR THREAT FOR ENTERPRISES ECONOMIC SECURITY

В умовах гібридної війни, тотального використання засобів масової інформації та її комунікаційних складових особливої актуальності набуває попередження основних загроз кіберзлочинності. Як свідчать результати наукових досліджень проблематика кіберзлочинності непокоїть не тільки державу в цілому, а й кожного окремо взятого господарюючого суб'єкта. Одразу ж зауважимо, що кіберзлочинність – неминучий наслідок глобалізації інформаційних процесів і як наслідок є основною загрозою соціогуманітарної компоненти підприємств. Зростаюча кількість кіберзлочинної діяльності на підприємствах, постійне вдосконалення інформаційних технологій і, як наслідок, нові можливості "вдосконалення" інструментів їх скоєння створюють економічні загрози для глобальних інформаційних мереж та соціогуманітарної компоненти.

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 %. До того ж самостійним видом злочинних дій стало викрадення ідентифікаційних даних інших осіб, використовуючи які, правопорушники набувають доступ до чужих банківських рахунків, безоплатно отримуючи послуги Інтернет-провайдерів та операторів зв'язку. Звертаємо увагу на те, що такі злочини характеризуються високим рівнем технічного забезпечення, латентністю, організованістю, наявністю міжрегіональних та міжнародних зв'язків [3].

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. При цьому ціннісний комплекс даної соціогуманітарної субкультури служить для легітимації і популяризації ідеї хакерства в суспільстві, саме тому людина, яка розділяє цінності хакерів, готова піти на інтернет-злочин, або схвалює злочини, що здійснюються іншими [1].

Вважаємо доцільно акцентувати увагу на тому, що кіберзлочинність має наслідки як на макро-, так і мікрорівнях, оскільки здатна спричинити значну шкоду окремому суб'єкту, в тому числі й господарської діяльності. Останнім часом відзначається значне зростання кількості випадків несанкціонованого втручання в інформаційні системи підприємств різних галузей. При цьому зловмисники блокують використання програмного забезпечення, що робить неможливою подальшу роботу різних підрозділів підприємства. Часто це призводить до виникнення проблем із контрагентами, контролюючими органами, оскільки тоді втрачається здатність обліково-аналітичної служби підприємства формувати інформацію, і зокрема звітну, та

вчасно її подавати у відповідні інстанції, а це, своєю чергою, призводить до застосування штрафних санкцій за порушення дисципліни платника податків.

Дослідження наукової проблематики, дозволяють виділити основні проблемні аспекти протидії кіберзлочинній діяльності в системі економічної безпеки підприємств: необхідність глобального обміну інформацією в режимі реального часу; приватному та державному секторам потрібні фінансове стимулювання для поліпшення кібернетичної безпеки; правоохоронним органам по боротьбі з транскордонною кіберзлочинністю потрібно більше повноважень; необхідна методичні напрацювання та впровадження у технології боротьби з кіберзлочинністю кращих практик інститутів міжнародної безпеки; існуюче дипломатичне упорядкування глобальних кібердомовленостей повинне стати більш адресованим; для допомоги громадянам потрібно удосконалити та розширити мережу кампаній з інформування населення про методи захисту від кібератак [2]. Така ситуація корелюється з перерахованими вище проблемами та свідчить про те, що збільшення рівня захищеності інформації в нашій країні потребує підтримки і розвитку.

Підводячи підсумки зазначимо, що для комплексної протидії кіберзлочинності з метою зміцнення економічної безпеки підприємств необхідні: 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.

Оскільки жодна держава не може захистити себе, вживаючи заходів тільки на національному рівні, Отже, у середовищі, де постійно з'являються та еволюціонують кіберзагрози, не можна залишатися незахищеним, оскільки сформована в світі ситуація зобов'язує до постійного вдосконалення методів боротьби з кіберзлочинами та стимулює побудову державної моделі, спрямованої на забезпечення кібербезпеки підприємств та зміцнення соціогуманітарної компоненти. 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.

Список використаних джерел:

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

2. Орлов О. В. Актуальні напрями державної політики у сфері боротьби з кіберзлочинністю / О. В. Орлов, Ю М.Онищенко // Теорія та практика державного управління. – Вип. 3 (42) – 2013 – с.1-6

3. 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.