КІБЕРЗЛОЧИННІСТЬ У ФІНАНСОВІЙ СФЕРІ УКРАЇНИ

А. Г. Коротунова, *здобувач вищої освіти групи Б-З/1*
обліково-фінансовий факультет, МНАУ

Останнім часом проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібернетичних шахраїв сягнули десятків мільярдів доларів. Серед найбільш вразливих до кібернетичних злочинів сфер суспільного життя відноситься фінансовий сектор економіки.

Аналіз національного законодавства у сфері протидії кіберзлочинності виявив, що в Україні чітко не визначено наступні поняття: кіберзлочинність, кіберзлочинець, кіберпростір, кібербезпека, кіберзахист. Разом з тим, застосовується диверсифікація дефініцій, не погоджених між собою. Так, в Законах України «Про боротьбу з тероризмом» [1] та «Про національну безпеку» [2] не прописуються ключові поняття, зокрема «комп'ютерний тероризм». У рішенні Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» кібербезпека

розглядається в контексті необхідності розробки і впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, в тому числі відповідно до вимог ратифікованої Верховною Радою України Конвенції про кіберзлочинність [3].

Останнім часом поширення набули такі види злочинів: кіберзлочинність у фінансово-банківській сфері; шахрайство з використанням платіжних карток та їх реквізитами; крадіжки коштів з банківських рахунків; «відмивання» грошей; заволодіння конфіденційною комп'ютерною інформацією про клієнтів тощо. Кібернетична злочинність все більше посягає на банківські рахунки як компаній чи організацій, так і пересічних громадян. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. Чинниками, які сприяють зростанню кіберзлочинів, є розвиток та удосконалення IT-технологій, значна географія для скоєння злочинів, недостатня теоретична та практична підготовка працівників органів внутрішніх структур та недосконаліть вітчизняного законодавства. Програм, за допомогою яких шахраї відбирають гроші у населення і банків, безліч, в т. ч. і шкідливі носії, такі як віруси Gamker і Carberp, банківські трояни для крадіжки інформації. Вірус вражає системи і краде інформацію з онлайн-банкінгу, публічні та приватні ключі, криптографічні утиліти та додатки, пов'язані з фінансами. Він здатний перехоплювати натискання клавіш і зберігати комбінації в окремий файл. Вірус також зберігає скріншоти і записи командного рядка, після чого посилає всі дані кіберзлочинцям [4].

Для протидії кіберзлочинам в державі створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюють, а технічні можливості посилюють. В Україні Департамент по боротьбі з кіберзлочинністю МВС України було створено у грудні 2011 р. (його сучасна назва Департамент кіберполіції Національної поліції України [4]).

Також існує міжнародний урядовий орган Міжнародна група з протидії відмиванню брудних грошей (FATF). Даний орган відстежує процеси

імплементації, вивчає способи і техніку відмивання грошей, розробляє превентивні та запобіжні заходи, сприяє загальносвітовій імплементації стандартів боротьби з відмиванням грошей. Виконуючи зазначені функції, міжнародна група плідно співпрацює з багатьма міжнародними організаціями, чия діяльність також спрямована на протидію відмиванню «брудних» грошей. Спочатку пріоритетом органу була боротьба з відмиванням доходів, отриманих від торгівлі наркотиками. Сьогодні їх діяльність має три головних напрямки: розширення дії прийнятих нею рекомендацій на всі континенти і регіони земної кулі; перевірка того, як виконуються в державах-членах і як впроваджуються в інших державах заходи для боротьби з відмиванням грошей, засновані на 40 рекомендаціях, які є керівництвом до дії; відстеження загальносвітових методів і схем відмивання злочинно нажитих капіталів та розробка контрзаходів [6-7].

Ключовим документом Міжнародної групи з протидії відмиванню брудних грошей (FATF) є рекомендації, які викладені у формі щорічних звітів організації. Дослідження проблем боротьби з кіберзлочинністю показали, що використання тільки технічного захисту інформації не має значного успіху. Кіберзлочинність є порівняно новою небезпекою для суспільства, але, на відміну від традиційних крадіжок і шахрайства, вона удосконалюється разом з технологіями, що ускладнює її виявлення та протидію [5].

Отже, явище кіберзлочинності має досить велику суспільну небезпечність. Про це говорять такі фактори як: стрімке зростання кількості вчинюваних кіберзлочинів; можливість завдання шкоди як фізичним, так і юридичним особам, і навіть державним структурам; досить складні способи захисту, і складність застосування найпростіших з них пересічними громадянами через неосвіченість у даній сфері тощо. Зауважимо, що є способи підвищити рівень кібербезпеки як країни в цілому, так і кожної конкретної людини, а саме: вдосконалення норм і прав боротьби з кіберзлочинністю; чітке розмежування компетенції та функцій правоохоронних органів; покращення практичного досвіду працівників підрозділів кіберполіції України; поліпшення

методичного забезпечення розслідування кіберзлочинів; налагодження співпраці зі службою безпеки банків та підприємств, судовою системою.

Література:

1. Про боротьбу з тероризмом : Закон України від 20 березня 2003 року № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 10.02.2019).

2. Про національну безпеку : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 12.02.2019).

3. Стратегія національної безпеки України: указ Президента України від 6 травня 2015 року № 287/2015. URL: http://zakon2.rada.gov.ua/laws/show/287/2015 (дата звернення : 12.02.2019).

4. Некрасов В. Экономическая правда. Легкие деньги: Украина превращается в Мекку для киберпреступников. Киев : Летопись, 2016. Т. 2 : Д–Й. С.34.

5. Група з розробки фінансових заходів боротьби з відмиванням грошей – FATF. URL: http://www.fiu.gov.ua/content/uk/fatf.htm.

6. Полторак А. С. Архітектоніка наслідків глобалізаційних процесів у фінансовій сфері. *Modern economics*, 2018. № 10. С. 89–96. https://doi.org/10.31521/modecon.V10(2018)-15.

7. Baryshevska I., Poltorak A., Shyshpanova N. Methodological approaches to assessing the state of fiscal decentralization. Social and economic aspects of sustainable development of regions : monograph. Opole (Poland) : The Academy of Management and Administrations in Opole, 2018. pp. 123–128.

Науковий керівник – **Полторак А. С.,**
канд. екон. наук, доцент кафедри фінансів, банківської справи та страхування
Миколаївський національний аграрний університет