5. Петренко К. В. Принципи та фактори регулювання соціогуманітарного розвитку депресивного регіону / К. В. Петренко // Проблеми економіки. – № 2, 2013 – С.127-131.
6. Чернюк Л. Г. Системна трансформація простору та її прояв як регулятора структури продуктивних сил / Л. Г. Чернюк, Т. В. Пепа // Збірник наукових праць ВНАУ. – Серія: Економічні науки. – №4 (81), 2013 – С.296-308.

УДК 343.97

Карапетян О. М.
к.екон.н., доцент кафедри
економічної безпеки та фінансових
розслідувань ЮФ ТНЕУ
Скакун Т. О.
студентка, ЮФ ТНЕУ

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: ПРАВОВІ КОЛІЗІЇ ТА ПРОБЛЕМИ МОНІТОРИНГУ

Сучасними викликами та актуальними проблемами сучасності є підвищення рівня кібербезпеки в Україні.

Аналіз національного законодавства у сфері протидії кіберзлочинності показав, що в Україні не визначено ряд таких ключових понять як: кіберзлочинність, кіберзлочинець, кіберпростір, кібербезпека, кіберзахист.

Разом з тим, застосовується диверсифікація дефініцій часто-густо не погоджених між собою. Так, в Законі України «Про основи національної безпеки України» згадуються «комп'ютерна злочинність» і «комп'ютерний тероризм», причому жоден з цих термінів не має свого визначення в даному нормативному документі [1].У Законі України «Про боротьбу з тероризмом» 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 [2].

У Доктрині інформаційної безпеки України затвердженої указом Президента України від 25 лютого 2017 року № 47/2017 згадуються «комп'ютерна злочинність» і «комп'ютерний тероризм», проте відсутні пояснення або посилання на такі пояснення. Крім того, в Доктрині згадуються і «кібератаки» без визначення терміну. Отже, можна констатувати, що національна нормативно-правова база в сфері інформаційної (кібернетичної) безпеки має суттєві недоліки [3].

Підґрунтям щодо кіберзлочинів є передбачені кримінальним законом суспільно небезпечні діяння і закріплені в окремому розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів),

систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. З точки зору кримінального права до кіберзлочинів відносяться тільки злочину, передбачені розділом XVI КК України [4].

Разом з тим, кіберзлочинність набуває все більшого масштабу, новітні технології дозволяють злочинцям залишатися анонімними та сприяють швидкому збагаченню шляхом злочинної діяльності.

Визначення кіберзлочинності залежить від того в якій сфері та з якими цілями здійснюються певні дії. Розповсюдженими злочинами кіберпростору є крадіжки інновацій або технологій, а також крадіжка грошових ресурсів. Найбільш гостро серед питань кіберзлочинів стоїть питання про злочини в банківській сфері, а саме доступ до коштів клієнтів банку.

Національний банк України виділяє такі види кіберзлочинів:

– банкоматне шахрайство;
– шахрайство в мережі Інтернет;
– шахрайство в системах дистанційного банківського обслуговування;
– шахрайство в торгівельно-сервісних мережах.

Протидія кіберзлочинам поєднує ряд заходів, серед таких слід визначити наступні: правові, технічні, організаційні та інформаційні. Однак ефективна протидія відмиванню злочинних доходів та зниження рівня кіберзлочинності можливі завдяки своєчасному виявленню фінансових операцій, які можуть бути пов'язані з відмиванням доходів, отриманих у сфері кіберзлочинності [5].

В Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» чітко визначено термін фінансовий моніторинг − сукупність заходів, які здійснюються суб’єктами фінансового моніторингу у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, що включають проведення державного фінансового моніторингу та первинного фінансового моніторингу [6].

У процесі забезпечення ефективності фінансового моніторингу необхідно визначити цілі, які будуть досягнуті в процесі використання певного напряму, а також доцільно чітко встановити ряд питань, необхідних для досягнення цілі.

Для підвищення рівня фінансового моніторингу доцільно дотримуватись таких принципів як: верховенство права, об'єктивності, незалежності, конфіденційності. Слід зазначити, що фінансовий моніторинг здійснюється в два етапи. Перший полягає в тому, що на даному етапі здійснюється виявлення операцій, які пов'язані із легалізацією доходів отриманих злочинним шляхом. При цьому застосовується порівняння із нормативно встановленими ознаками операцій такого типу. Другий етап полягає в перевірці даної інформації щодо зв'язку фінансових операцій з легалізацією доходів, здобутих злочинним шляхом [7].

Для здійснення фінансового моніторингу відповідальні працівники змушені попередньо опрацювати можливі механізми та способи здійснення кіберзлочинів у сфері відмивання незаконних доходів. Злочинці, які працюють у сфері кіберзлочинності, для відмивання злочинних доходів використовують різні механізми та інструменти. Серед них можна назвати наступні:

– використання рахунків, відкритих особами за втраченими документами, на підставних осіб;
– використання альтернативних платіжних систем (електронні платежі);
– купівля електронних грошей та використання систем платежів через електронні гаманці;
– конвертація незаконних доходів у товари шляхом придбання останніх через мережу Інтернет;
– проведення ланцюга фінансових операцій через декілька банківських рахунків за допомогою віддаленого доступу [8].
– Для виявлення схем відмивання доходів, отриманих злочинним шляхом здійснюється фінансовий моніторинг спеціально уповноваженими на те органами. Зокрема повинні здійснюватись такі заходи:
– виїзні перевірки (дають можливість на місці вивчити необхідні документи);
– оперативні заходи (обшук, допит);
– аналіз звітності (фінансова звітність, податкова звітність та ін.);
– дослідження фінансової операції (збір інформації та аналіз операцій);
– валютний контроль (здійснюється банківськими установами та іншими агентами валютного контролю при проведенні розрахунків у іноземній валюті, вивезенні/ввезенні, переказуванні і пересиланні валютних цінностей, в тому числі розміщення валютних цінностей на рахунках і у вкладах за межами України, інших валютних операцій) [9].

Підсумовуючи вищесказане, зазначимо, що для підвищення ефективності моніторингу у сфері кіберзлочинності доцільно створити уніфіковану класифікацію і формальну модель кіберзлочинців, що полегшить роботу з протидії кіберзлочинності.

ЛІТЕРАТУРА:

1. Про основи національної безпеки України [Електронний ресурс]: Закон України від 19 червня 2003 року № 964–IV // Верховна Рада України. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15
2. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» [Електронний ресурс]: Указ Президента України від 6 травня 2015 року № 287/2015. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015
3. Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України» [Електронний ресурс]: Указ Президента України від 25 лютого 2017 року №47/2017. − Режим доступу: http://zakon3.rada.gov.ua/laws/show/47/2017
4. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III [Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2341-14.
5. Кіберзлочинність та відмивання коштів [Електронний ресурс]: Державна служба фінансового моніторингу України. – Режим доступу: http://www.sdfm.gov.ua/content/file/site_docs/2013/20131230/tipolog2013
6. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення [Електронний

ресурс]: Закон України від 14 жовтня 2014 року // Верховна Рада України. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/1702-18
7. Буткевич С. А. Фінансовий моніторинг як гарантія економічної безпеки держави: зарубіжний та вітчизняний досвід. [Електронний ресурс] / С. А. Буткевич. – Режим доступу: file:///C:/Users/Таня/Downloads/VKhnuvs_2008_43_43.pdf
8. Кузнецова, С.А. Фінансовий моніторинг в Україні: якісний аспект. [Електронний ресурс] / С.А. Кузнецова. – Режим доступу: http://bo0k.net/index.php?p=achapter&bid=5377&chapter=1
9. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом «Властивості та ознаки операцій, пов'язаних з відмиванням коштів шляхом зняття готівки. Тактичне дослідження та практичне розслідування». [Електронний ресурс] / Державна служба фінансового моніторингу України. – Режим доступу: http://www.sdfm.gov.ua/articles.php?cat_id=114&art_id=1890&lang=uk

УДК 004.056.5

Колесніков А. П.
к.е.н., доцент кафедри економічної
безпеки та фінансових розслідувань
ЮФ ТНЕУ

ТЕНДЕНЦІЇ КІБЕРБЕЗПЕКИ В УМОВАХ ЗОВНІШНІХ І ВНУТРІШНІХ ВИКЛИКІВ

В час глобальної інформатизації суспільства приватна і публічна безпека знаходиться під динамічно змінюваними загрозами.

Глобалізація застосування сучасних інформаційних та комунікаційних технологій у всіх сферах життя суспільства, державних і недержавних структур супроводжується випереджаючим виникненням кіберзагроз і їх матеріалізації.

Новітність загроз інформаційному простору, поглиблена умовами асиметричної війни, визначає необхідність глибшої ідентифікації загроз кібербезпеці та окреслення засобів та інструментів боротьби з ними.

Множинність і постійна динаміка векторів кіберзлочинності ускладнює розробку універсальної їх класифікації. Типовим підходом є запропонований у Конвенції про кіберзлочинність Ради Європи, у якій виокремлено наступні види правопорушень: злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем; злочини, пов'язані з комп'ютерами; злочини, пов'язані з контентом; злочини, пов'язані з правами власності [2].

В розвинених країнах економічні збитки від прогресування кіберзлочинності вимірюються дуже значними сумами. За даними Інтерполу втрати економік Європи від кіберзлочинців щорічно складають 750 мільярдів євро [1]. За статистикою організації LACNIC, що займається аналізом Інтернет-активності щорічні втрати США від кіберзлочинності складають від20 до 140 млрд. доларів, або близько 1% від ВВП країни, а в Латинській