УДК 004.056.5

Андрій Колесніков,
кандидат економічних наук, доцент кафедри економічної безпеки та фінансових розслідувань Тернопільського національного економічного університету

Марія Зяйлик,
кандидат економічних наук, доцент кафедри менеджменту у виробничій сфері Тернопільського національного технічного університету імені Івана Пулюя

ЕКОНОМІКО-ПРАВОВІ ЗАСАДИ РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ ТА МЕТОДІВ БОРОТЬБИ З НЕЮ

Уточнено дослідження проблематики визначення сутності кібербезпеки з урахуванням правової компоненти наказовості за кіберзлочини. Визначено основні ознаки суттєвого загострення загроз кіберзлочинності в Україні. Окреслено загрози для України в контексті посилення боротьби з кіберзлочинністю у світі.

Ключові слова: *кіберзлочинність, кібербезпека, кібершахрайство, передумови кіберзлочинності в Україні.*

Колесников А., Зяйлык М.
Экономико-правовые основы развития киберпреступности и методов борьбы с ней
Уточнено исследования проблематики определения сущности кибербезопасности с учетом правовой компоненты наказуемости за киберпреступления. Определены основные признаки существенного обострения угроз киберпреступности в Украине. Определены угрозы для Украины в контексте усиления борьбы с киберпреступностью в мире.

Ключевые слова: *киберпреступность, кибербезопасность, кибермошенничество, предпосылки киберпреступности в Украине.*

Kolesnikov A., Zyaylyk M.
Economic and legal basis of development the cybercrime and the methods of fighting it
In the article it is refined the research on issues of defining the essence of cyber security considering legal component of punishment by law for cybercrime. The main characters of significant exacerbation the threats of cybercrime in Ukraine are determined. It is outlined the threats to Ukraine in the context of strengthening the fight against cybercrime in the world.

Keywords: *cybercrime, cyber security, cyber fraud, backgrounds of cybercrime in Ukraine.*

Постановка проблеми. 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. Такі інструменти мають охоплювати комплекс організаційних, економічних та правових механізмів протидії.

Аналіз останніх досліджень і публікацій. Дослідження термінологічної сутності та сучасних тенденцій розвитку кіберзлочинності і методів боротьби з нею здійснювали О. Баранов [6], В. Бурячок [8; 9], О. Корченко [9], О. Шаховал, І. Лозова, С. Гнатюк [4], О. Вівчар [10; 11].

Цілями даної статті є поглиблення аспектів розвитку кіберзлочинності в Україні та окреслення економіко-правових засад протидії кіберзагрозам.

Виклад основного матеріалу дослідження. Дослідження аспектів кіберзлочинності та кібербезпеки України передбачає вивчення категорійного апарату та його динаміки в умовах вітчизняної та світової кіберстратегій. Охарактеризувавши шість аспектів досліджуваного об'єкту, О. А. Баранов визначив, що кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави

в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [6, с. 61]. Разом з тим значна охоплюваність у визначенні об'єктів кібербезпеки не повністю передбачає аспектів кримінальної та цивільної відповідальності за акти кіберзлочинності. Так, категорія негативного інформаційного впливу в чинному законодавстві не передбачена, однак відповідальність за доведені факти антиреклами передбачена статтями 28 (Публічне спростування недобросовісної та неправомірної порівняльної реклами) та 29 (Права об'єднань громадян, об'єднань підприємств у галузі реклами) Закону України «Про рекламу» [7]. Зрозуміло, що такий приклад є не всеохопним, а лише одним з аспектів.

Елемент «негативні наслідки функціонування інформаційних технологій» також варто уточнити з правової точки зору. Раціональним вважаємо трактування «незаконні дії з платіжними картками та іншими технічними та інформаційними засобами з метою отримання особистої вигоди або спричинення шкоди стороннім особам чи суб'єктам господарювання». Згадування у визначенні платіжних карток як прикладу зумовлено активним розвитком даного виду кіберзлочинності в Україні за останні роки. В такому разі відповідальність за такі злочини передбачена статтями 200 (Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення) та 232 (Незаконне використання інсайдерської інформації) Кримінального кодексу України [5].

Врахування зазначених рекомендацій поглибить правовий аспект обґрунтованого визначення.

Множинність і постійна динаміка векторів кіберзлочинності ускладнює розробку їх універсальної 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 млрд. євро [1]. За статистикою організації LACNIC, що займається аналізом Інтернет-активності, щорічні втрати США від кіберзлочинності складають від 20 до 140 млрд. доларів, або близько 1% від ВВП країни, а в Латинській Америці фінансові втрати від діяльності кіберзлочинців склали 1,1 млрд. доларів [3].

Зведені дані щодо втрат економіки України від кіберзлочинців відсутні, однак про їх масштаби свідчать оцінки експертів Kaspersky Lab, які сформулювали перелік загроз, що роблять Україну однією з головних «гарячих точок» на кіберкарті світу [3]. Це стало результатом абсолютного лідерства за кількістю внутрішніх і зовнішніх кіберзагроз в Європі. За останні роки наша держава неодноразово ставала жертвою не тільки для дрібних шахраїв, але і для широкомасштабних кібероперацій найвищого рівня.

Результати ряду досліджень свідчать про низьку ефективність вітчизняних методів боротьби з кіберзлочинністю і недостатню практику їх здійснення. Серед ознак та передумов суттєвого загострення загроз кіберзлочинності виокремлюють:

1. Деградація науково-технічного потенціалу України та нерозвиненість національної інноваційної системи в сфері інформаційної безпеки.

2. Значну вразливість інформаційної сфери України через надмірно широке використання матеріально-технічних засобів іноземного виробництва [8].

3. Низька захищеність користувачів програмного забезпечення від вірусних атак внаслідок його неоновлення чи використання піратських копій.

4. Поширення спаму з проханнями допомоги від імені українських інтернет-користувачів, спекулюючи складним економічним, політичним та безпековим становищем в країні.

5. Україна посідає перші місця у рейтингах світу за ризиками зіткнення з веб-загрозами. Майже третина українських користувачів мережі зіткнулися із загрозами, що поширюються через Інтернет.

6. Україна має найбільший ризик зараження шкідливими мобільними застосунками. Досить високий для українців і ризик зіткнення з локальними загрозами, до яких відносяться об'єкти, що проникли на комп'ютери шляхом зараження файлів, знімних носіїв або спочатку потрапили на комп'ютер не у відкритому вигляді (наприклад, ПЗ в складі складних інсталяторів, зашифровані файли і т. д.).

7. В Україні виявлено значну кількість шкідливого програмного забезпечення (програм-вимагачів чи шифрувальників), що розроблене для блокування пристроїв або браузерів чи шифрування файлів користувача недоступними для нього кодами з метою подальшого отримання викупу за передачу ключа коду.

8. Комп'ютери українських чиновників стали жертвами однієї з найскладніших кібершпигунських кампаній Turla. Це угрупування здійснило зараження сотні комп'ютерів більш, ніж в 45 державах світу, які є власністю державних установ.

9. Українці були серед жертв таких кампаній, як: CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy і Red October [4, 57–58].

За даними Української міжбанківської асоціації членів платіжних систем ЕМА, у 2015 р. було зроблено 257 спроб списання коштів з рахунків клієнтів банків (їх загальна сума 108 700 000 грн.). Результати цих злочинів фактично не розслідуються через низьку розробленість правового механізму захисту.

Ще однією проблемою є низький рівень правового захисту громадян при здійсненні інтернет-покупок через відповідні сайти.

Складністю досягнення Україною стану кібербезпеки є як недостатня кількість державних експертів в сфері комп'ютерно-технічної експертизи, так і складнощі з введенням в правове поле досліджень фахівців.

Важливою проблемою в протидії кібершахрайству є низький рівень обізнаності українських громадян у питаннях безпеки та конфіденційності інформації.

Серед реалізованих контрзаходів світової спільноти для протидії кібертероризму визначимо наступні:

− 2009 р. – введення в США посади Національного радника щодо кібербезпеки;

− 2011 р. – заснування у Великобританії Міжнародного альянсу забезпечення кібербезпеки;

− 2009 – 2013 рр. – створення підрозділів кібервійськ у КНР, США, Росії (зародження створення аналогічних служб в Україні), організація агентств кібероборони у Австрії (APCIP), Великобританії (CPNI), Німеччині (NCAZ), Швейцарії (MELANI) та Нідерландах (NICC), а також включення вимог щодо забезпечення кібербезпеки у ключові нормативні документи критично важливих галузей народного господарства [9, с. 43].

Глобальна програма кібербезпеки передбачає реалізацію наступних засад: правові; технічні й процедурні; організаційні; створення потенціалу; міжнародна співпраця [12]. Поряд з вагомістю усіх зазначених засад вагомість і обґрунтованість правових рішень є одими з базових. Ці рішення передбачають фахове застосування основних положень карного законодавства на предмет відповідальності за ряд таких злочинів, як: комп'ютерне шахрайство, незаконний доступ, спотворення даних, порушення авторських прав і дитяча порнографія. Методи та механізми розслідування кіберзлочинів, зважаючи на технічну та просторову специфіку їх здійснення, змістово суттєво відрізняються від карних злочинів загального характеру. Міжнародні масштаби боротьби з кіберзлочинністю передбачають уточнення і гармонізацію національного законодавстваз тим, щоб мати можливість спільної співпраці з правоохоронними органами за кордоном.

Недотримання даних принципів та посилення правового та технічного захисту від кіберзлочинності в ЄС і США потенційно переорієнтує кіберзлочинців на країни з менш розвиненою системою захисту, в тому числі і в Україну. Разом з тим, кібербезпека не може бути досягнута лише за рахунок технічних засобів. Парадокс полягає в тому, що в період надінтенсивної інформатизації суспільства підвищення складності програмного забезпечення підвищує і його вразливість, знижує ефективність традиційних організаційних заходів і засобів інженерного та технічного захисту інформації в комп'ютерних та інформаційних системах, зокрема стосовно несанкціонованого доступу до комп'ютерів та мереж.

Нормативно-правовою основою протидії кіберзлочинності на національному рівні є Кримінальний кодекс України, в якому окремі види комп'ютерних злочинів виокремлено в розділ VI Особливої частини – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361, 363)». Окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину, розміщені в інших розділах.

В Розділі V Особливої частини зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину (ст. 163, 176, 177) та злочини у сфері господарської діяльності (ст. 200) в Розділі VII [5].

Висновки. Описані приклади свідчать про низьку ефективність сучасної системи кібербезпеки України і першочергову потребу її удосконалення та оптимізації. Досягнення цього вирішить не тільки проблему безпеки інформаційного простору, але і забезпечить безперервність та сталість розвитку економіки України.

Список використаної літератури

1. *Европа объявила войну киберпреступности / [Електронний ресурс]. – Режим доступу : http://www.dw.de/европа-объявила-войну-киберпреступности/a-15988857-1.*
2. *Конвенція про кіберзлочинність / [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575.*
3. *Финансовые потери от киберпреступности в Латинской Америке превысили $1 млрд. / [Електронний ресурс]. – Режим доступу : http://itar-tass.com/mezhdunarodnaya-panorama/1001716.*
4. *Шаховал О. Рекомендації щодо розробки стратегії кібербезпеки України / О. Шаховал, І. Лозова, С. Гнатюк // Захист інформації. – 2016. – № 1. – С. 57–65.*
5. *Кримінальний кодекс України / [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2341-14.*
6. *Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов // Правова інформатика. – 2014. – №2. – С. 54–62.*
7. *Про рекламу. Закон України № 271/96-ВР від 03.07.1996 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80/page.*
8. *Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / В. Л. Бурячок // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С. 104–114.*
9. *Корченко О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Корченко, В. Бурячок, С. Гнатюк // Ukrainian Scientific Journal of Information Security. – 2013. – № 19 (1). – С. 40–44.*
10. *Vivchar O. Contemporary pragmatics and vectors of combating cybercrime in the context of information and economic security strengthening / O. Vivchar // Актуальні проблеми правознавства. – 2017. – № 1. – С. 27–30.*
11. *Вівчар О. І. Соціогуманітарний вимір: кіберзлочинність як основна загроза економічній безпеці підприємств / О. І. Вівчар // Матеріали Шостої Всеукраїнської наук.-практ. конф. пам'яті почесного професора ТНТУ, академіка НАН України Чумаченка Миколи Григоровича «Інноваційний розвиток: стратегічний погляд у майбутнє». ТНТУ імені Івана Пулюя, Тернопіль, 6 квітня 2017 року. – С. 18–19.*
12. *Глобальная программа кибербезопасности (ГПК) МСЭ / [Електронний ресурс]. – Режим доступу : www.ifap.ru/pr/2008/080908aa.pdf.*

Стаття надійшла до редакції 14.04.2017.