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

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 причин суттєвого загострення загроз кіберзлочинності виокремлюють [4, 57-58]:

1. Низька захищеність користувачів програмного забезпечення від вірусних атак внаслідок його не оновлення чи використання піратських копій.

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

3. 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.

4. 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.).

5. 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.

6. 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.

7. Також українці були серед жертв таких кам-паній, як CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy і Red October.

За даними Української міжбанківської асоціації членів платіжних систем ЕМА, у 2015 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.

Проблемою України 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.

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 і знижує ефективність традиційних організаційних заходи 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

Особливої частини. 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].

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.

ЛІТЕРАТУРА:

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. Шахова, 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