

ційно-технічних питань, пов'язаних із забезпеченням скоординованого формування та ведення інформаційних ресурсів всієї діяльності господарюючих суб'єктів.

1. Твердохліб М. Г. Інформаційне забезпечення менеджменту: Навч. посібник / М.Г. Твердохліб. — [Вид. 2-ге, доп. та перероб.]. — К.: КНЕУ, 2006. — 224 с.
2. Черешкин Д.С. Оружие, которое может быть опаснее ядерного / Д.С. Черешкин // Независимая газета. — 2007. — № 123.
3. Демкова М. Інформація як основа інформаційного суспільства: визначення поняття та правове регулювання / М. Демкова, М. Фігель // Інформаційне Суспільство. Шлях України. — К. : Фонд «Інформаційне суспільство України», 2004. — 422 с.
4. Юридична енциклопедія: В 6 т. // Редкол.: Ю.С.Шемшученко (голова редкол.) та ін. — К. : Укр. енцикл., 1998. — С. 717.
5. Беккер Л.М. Воспитание и основы его моделирования / Л.М. Беккер. — М. — 286 с.
6. Дегтяр А.О. Державно-управлінські рішення: інформаційно-аналітичне та організаційне забезпечення: [Моногр.] / А.О. Дегтяр. — Х.: Вид-во ХарПІ НАДУ «Магістр». — 2006. — 224 с.

Кіберзлочинність у фінансовій сфері України

Шасвська Ю.В.,

курсант Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.,

завідувач кафедри кібербезпеки та інформаційного забезпечення

Одеського державного університету внутрішніх справ,

кандидат юридичних наук

Останнім часом проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібершахраїв сягнули десятків мільярдів доларів та постійно зростають. Серед найбільш вразливих до кіберзлочинів сфер суспільного життя відноситься фінансовий сектор економіки, а саме – банки та їх послуги [1].

Кіберзлочинність – це п'ятий за розмірами вид економічної злочинності в Україні після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю.

За результатами опитування на кіберзлочинність припадає 23% випадків шахрайства у світі і 17% в Україні (рис.1).



Рис. 1

З статичних даних ми бачимо, що у відсотковому співвідношенні рівень кіберзлочинності у світі вищий ніж в Україні. Це явище пояснюється тим, що фінансова сфера, яка досить часто потопає від кібератак, в Україні менш розвинена ніж у всьому світі, тому звідси й нищі показники. І це зовсім не з причин якісної організації протидія кіберзлочинцям.

Розглянемо причини розповсюдження кіберзлочинності:

- по-перше, зазначена сфера злочинна діяльності є дуже прибутковою та стає в один ряд з такими незаконними сферами діяльності, як незаконний обіг наркотиків, зброї та торгівля людьми;
- по-друге, фінансові установи скривають від правоохоронних органів більшість фактів кібератак на свої установи, піклуючись про свою репутацію серед клієнтів;
- по-третє, за умови незначних фінансових втрат, фінансові установи не проводять навіть внутрішніх розслідувань з огляду на те, що людські, фінансові та інші затрати на таке їх проведення значно перевищують втрати;
- по-четверте, злочини скоїться у віртуальному середовищі, тобто є дуже латентними.

Так, за оцінками експертів, в останні місяці тільки в м. Києві фіксується до двадцяти випадків крадіжки грошей через клієнт-банк в місяць. Суми становлять від 20 тис. до 40 млн. грн. Однак

подібні факти замовчуються, повідомлень в ЗМІ про них практично немає. Ні потерпілим, ні банкам не вигідний галас навколо того, що відбувається. У ряді випадків бувають ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків [2].

На сьогодні кіберзлочинність – це реальна глобальна загроза, яка може походити з будь-якої країни світу і виходити за межі конкретної юрисдикції на відміну від багатьох інших традиційних видів економічних злочинів.

Серед усіх сфер суспільного життя найбільш вразливою до шахрайства є фінансово-кредитна сфера, особливо у міжнародних економічних відносин.

Останнім часом найбільшого поширення набули такі види злочинів як кіберзлочинність в 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 ІТ-технологій, значна географія для скоєння злочинів, недостатня теоретична та практична підготовка працівників органів внутрішніх структур та недосконалість вітчизняного законодавства [3].

Так, в опитуванні представлені погляди представників понад 13 різних галузей. Фінансові послуги, роздрібна торгівля, виробництво споживчих товарів, промислове виробництво та професійні послуги представляють понад половину (63%) від загальної кількості учасників в Україні та світі. Кожен другий респондент, що працює у секторі фінансових послуг, енергетики та гірничо-видобувної промисловості за останні 12 місяців зіштовхнувся із випадками кіберзлочинів (рис.2) [4].

Дослідження проблем боротьби з кіберзлочинністю показали, що використання тільки технічного захисту інформації не має значного успіху.

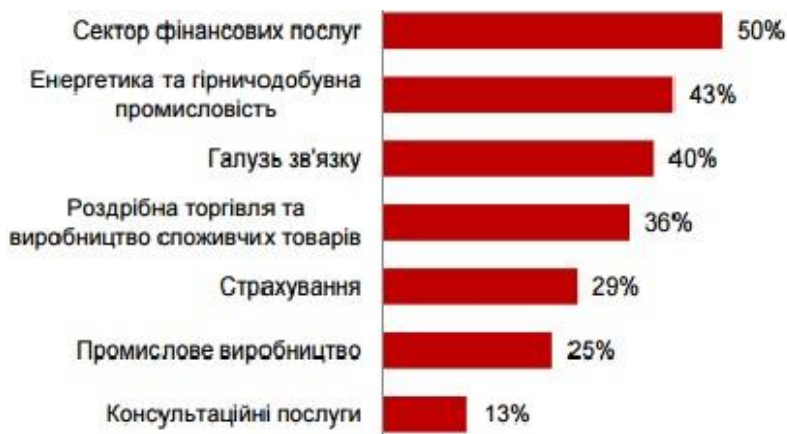


Рис.2

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, що унеможливорює складення єдиної методики та тактики розслідування зазначених злочинів.

За офіційними даними, більшість респондентів, які зіткнулися з економічною кіберзлочинністю злочинністю за останні 12 місяців, оцінюють збитки до 5 млн. доларів США.

Найдорожчими для організацій виявилася маніпуляції з фінансовою звітністю (рис. 3)



Рис. 3

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.

Наведемо кількість шахрайських операцій із використанням платіжних карток, емітованих українськими банками в 2010 – 2015 роках у вигляді діаграми (рис. 4)

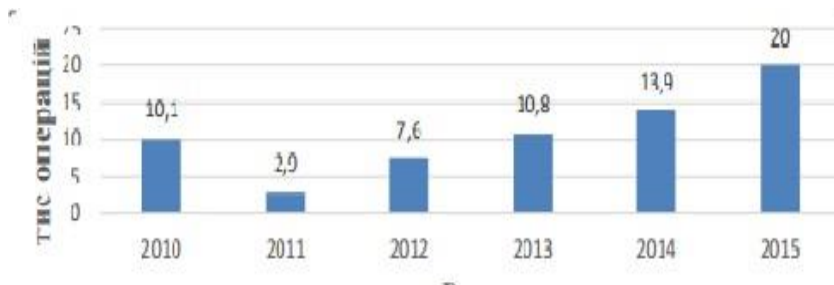


Рис. 4

Основні висновки щодо стану кіберзлочинності в Україні:

- кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні;
- кожен третій респондент (37%) вважає, що ризик кіберзлочинності підвищився за останні 12 місяців;
- понад 25% організацій не мають відповідних політик та механізмів реагування на кіберзлочини;
- 46% опитаних не проходили навчання в області кібербезпеки протягом останніх 12 місяців;
- 58% респондентів з України заявили, що в їхніх організаціях відсутній процес моніторингу відвідування соціальних мереж.

В Україні способами протидії кіберзлочинності можуть виступати: вдосконалення норм і прав боротьби з кіберзлочинністю, чітке розмежування компетенції та функцій правоохоронних органів. Також одним із способів протидії кіберзлочинності може бути покращення практичного досвіду працівників підрозділів кіберполіції України, поліпшення методичного забезпечення розслідування кіберзлочинів, налагодження співпраці зі службою безпеки банків та підприємств, судовою системою.

1. Чекотовська О. Правове регулювання кіберзлочинності. – [Електронний ресурс] / Ольга Чекотовська. – Режим доступу: <http://ukrjustice.com.ua>.
2. Кіберзлочинність в Україні. – [Електроннийресурс] – Режим доступу: <http://www.science-community.org>
3. Некрасов В. Экономическая правда / Всеволод Некрасов. Легкие деньги: Украина превращается в Мекку для киберпреступников . – Киев : Летопись, 2016. – Т. 2 : Д–Й. – С.34.
4. Дуброва Н.П., Сучасгтц стан фінансової системи України в глобалізаційному процесі // Фінансове право - 2015р. – №1(9) - с.114-115.
5. Коротких Я.В. Економічна безпека в умовах глобалізації // «Розвиток фінансової системи України». – 2016р. – с.211-212.