МОДЕЛЮВАННЯ СКЛАДНИХ СОЦІАЛЬНО-ЕКОНОМІЧНИХ СИСТЕМ

УДК 330.101.52:004

М.О. Дворнік

аспірант
Класичний приватний університет

СТАТИСТИЧНІ МЕТОДИ ОЦІНЮВАННЯ РІВНЯ КІБЕРЗЛОЧИННОСТІ НА ОСНОВІ ОПИТУВАННЯ ДОМОГОСПОДАРСТВ

У статті досліджено класифікацію кіберзлочинності, яка насамперед поділяється на злочини, пов'язані з комп'ютерними даними чи системою, та злочини, що вчиняються за допомогою комп'ютерної техніки. Висвітлено методи збору інформації щодо здійснення вказаних злочинів за видами, які поширюються не на всіх суб'єктів економічної діяльності. Запропоновано розробити анкету щодо всіх видів кіберзлочинності, яка, зокрема, буде поширюватися на домогосподарства.

Ключові слова: *кіберзлочинність, інформаційне суспільство, анкетування, Інтернет, комп'ютерна техніка, методи оцінювання.*

І. Вступ

У період розвитку інформаційного суспільства з'являється все більше можливостей діяльності за допомогою комп'ютерної техніки та мережі Інтернет, але водночас розвивається такий вид злочину, як кіберзлочинність, який, у свою чергу, створює великі економічні проблеми підприємствам, домогосподарствам та економічному розвитку країни в цілому. Тому дослідження проблематики збору даних щодо цього виду злочинів на сьогодні є актуальним, а розроблення методів оцінювання рівня кіберзлочинності на основі здійснення опитувань домогосподарств є необхідним.

ІІ. Постановка завдання

Метою статті є аналіз класифікацій кіберзлочинності й розробка статистичних методів оцінювання кіберзлочинності в Україні на основі опитування домогосподарств.

ІІІ. Результати

Окремі питання щодо способів розподілу злочинів у комп'ютерній сфері висвітлено в працях вітчизняних і зарубіжних науковців: В. Вєхова [1], А. Волобуєва [2], О. Россинської, О. Усова [3] та ін. Проблемам протидії правопорушенням у сфері використання інтернет-технологій присвячено чимало праць, але вони зосереджені на необхідності вдосконалення чинного законодавства, що регулює інформаційні відносини, зокрема розробки Інформаційного кодексу, розбудови відповідних організаційних структур правоохоронних органів для виявлення та розслідування цих специфічних видів злочинів, професійної підготовки спеціалістів для цих підрозділів тощо. Зазначені питання розглядають такі науковці, як: В. Бутузов, В. Гавловський, В. Голубєва, Р. Калюжний, Б. Романюк, В. Цимбалюк та ін. [6].

Науковець В. Вєхов комп'ютерні злочини умовно поділяв на дві основні групи, виходячи з класифікаційної ознаки категорії доступу до засобів комп'ютерної техніки:

1) внутрішні користувачі;

2) зовнішні користувачі, де користувач – суб'єкт, який звертається до інформаційної системи, або посередника, за отриманням необхідної йому для користування інформації.

А. Волобуєв виділяє три групи комп'ютерних злочинів:

1) злочини, в яких специфічні властивості комп'ютера виступають як безпосередній предмет посягань (розкрадання машинного часу, несанкціоноване втручання в процес обробки інформації, несанкціоноване використання комп'ютерної інформації, знищення комп'ютерних даних або програм, несанкціоноване копіювання комп'ютерних програм);

2) злочини, вчинені шляхом використання комп'ютерної системи як засобу досягнення злочинної мети;

3) злочини, пов'язані з комп'ютером.

О. Россинська та О. Усов пропонують таку класифікацію злочинів, пов'язаних з комп'ютерами:

1) злочини, предметом яких є комп'ютерні засоби;

2) злочини, в яких комп'ютерні засоби є одночасно і предметом, і засобом вчинення злочину;

3) злочини, в яких комп'ютерні засоби виступають як засоби вчинення й (або) укриття злочину;

4) злочини, в яких комп'ютерні засоби виступають як джерело криміналістично значущої інформації.

Сучасний світ практично неможливо уявити без інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства так чи інакше пов'язані з комп'ютерами, комп'ютерною мережею й комп'ютерною інформацією. Персональний комп'ютер, КПК, мобільний телефон з підключенням до Інтернету сприймається як належне й необхідне. Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказів коштів і багато іншого [4].

Разом із цим останнім часом в Україні значно зросла кількість інтернет-користувачів, тому що підключення до глобальної мережі стало доступним і зручним. Про це явище можна дізнатися з результатів дослідження GfK Ukraine, в яких показано, що кількість регулярних інтернет-користувачів старше 16 років в Україні зросла в I кварталі 2013 р. порівняно з IV кварталом 2012 р. на 15,1% (на 21% порівняно з I кварталом 2012 р.) і становила 17,34 млн осіб. За підсумками 2012 р. кількість регулярних інтернет-користувачів старше 16 років в Україні становила 15,41 млн осіб, що на 27% більше, ніж у 2011 р. [5].

Водночас із поширенням використання інтернет-технологій пропорційно зростає й загроза правопорушень, метою яких є хакерські атаки, викрадення персональної інформації, блокування роботи інформаційних служб, шантаж, шахрайство тощо. Це зумовлено низкою причин, зокрема зростанням довіри до електронних засобів обробки інформації, розширенням кола суб'єктів – учасників інформаційних відносин у глобальній мережі, збільшенням кількості різноманітних сервісів, переходу до обслуговування банківських установ. В Інтернеті сьогодні набули поширення різноманітні схеми, спрямовані на отримання коштів з недосвідчених і довірливих користувачів інтернет-магазинів, віртуальних аукціонів, сайтів знайомств тощо. Зазвичай для такого виду шахрайства використовуються інтернет-сайти, що візуально та за назвою нагадують відомі міжнародні ресурси. Проте, на відміну від добре зарекомендованих брендів, на отримання замовленого товару або повернення коштів годі й сподіватися. Причина користування такими ресурсами – бажання отримати замовлення за надзвичайно низькою ціною. Іноді зловмисники використовують і протилежні якості людини, наприклад, створюючи фіктивний сайт благодійного фонду або школи-інтернату [6].

З поширенням технологій змінився і характер злочинів. Якщо раніше більшість з них припадала на махінації з пластиковими картками, то тепер відбувається справжній бум у сфері онлайн-платежів. Найбільш професійні хакери вже перейшли у сферу крадіжок через клієнт-банки (системи дистанційного банківського обслуговування). Махінації з картками відходять на другий план, натомість збільшується кількість крадіжок з рахунків компаній або з електронних гаманців [7].

Поняття "комп'ютерна злочинність" уперше з'явилася в американській, а потім і в іншій іноземній літературі на початку 60-х рр. XX ст. "Комп'ютерна злочинність" – це порушення чужих прав та інтересів щодо автоматизованих систем обробки даних. За останні 10–15 років сформувалось поняття "кіберзлочинність", під якою розуміють злочинність у традиційному значенні цього слова, але яка наявна в мережі Інтернет [8].

Конвенція Ради Європи про кіберзлочинність говорить про чотири типи комп'ютерних злочинів "у чистому вигляді", визначаючи їх як злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

1. Незаконний доступ – ст. 2 (протиправний умисний доступ до комп'ютерної системи або її частини).

2. Незаконне перехоплення – ст. 3 (протиправне умисне перехоплення не призначених для громадськості передач комп'ютерних даних на комп'ютерну систему, з неї або в її межах).

3. Втручання в дані – ст. 4 (протиправне пошкодження, видалення, порушення, зміна або припинення комп'ютерних даних).

4. Втручання в систему – ст. 5 (серйозне протиправне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, видалення, порушення, зміни чи припинення комп'ютерних даних).

Саме ці чотири види злочинів є власне "комп'ютерними", решта – це або пов'язані з комп'ютером (computer-related), або вчинені за допомогою комп'ютера (computer-facilitated) злочини. До них належать: злочини, пов'язані з порушенням авторських і суміжних прав; дії, де комп'ютери використовуються як знаряддя злочину (електронні розкрадання, шахрайства тощо); злочини, де комп'ютери відіграють роль інтелектуальних засобів (наприклад, розміщення в мережі Інтернет дитячої порнографії, інформації, що розпалює національну, расову, релігійну ворожнечу тощо) [9].

Специфіка цього виду злочинності полягає в тому, що готування та вчинення зло-

чину здійснюється, практично не відходячи від "робочого місця", злочини є доступними; оскільки комп'ютерна техніка постійно дешевшає; злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати й вилучити криміналістично значущу інформацію при виконанні слідчих дій для використання її як речового доказу [4].

Окрім злочинів, дослідники класифікували комп'ютерних злочинців відповідно до вчинених ними злочинів:

а) порушники правил користування ЕОМ – вчинюють злочини через недостатнє знання техніки, бажання ознайомитися з інформацією, яка їх цікавить, викрасти будь-яку програму або безкоштовно користуватися послугами ЕОМ;

б) "білі комірці" – так звані респектабельні злочинці: бухгалтери, скарбники, керівники фінансів різних фірм. Для них характерні: використання ЕОМ із метою моделювання планованих злочинів, комп'ютерний шантаж конкурентів, фальсифікація інформації тощо. Мета їхніх дій – отримання матеріального зиску або приховування інших злочинів;

в) "комп'ютерні шпигуни" – добре підготовлені в технічному плані фахівці, метою діяльності яких є отримання стратегічно важливої інформації з різних галузей;

г) "хакери" ("одержимі програмісти") – найбільш технічно та професійно підготовлені особи, які відмінно знаються на обчислювальній техніці та програмуванні. Їхня діяльність спрямована на несанкціоноване проникнення в комп'ютерні системи, крадіжку, модифікацію або знищення наявної в них інформації. Найчастіше вони вчинюють злочини, не маючи на меті при цьому отримання прямого матеріального зиску [10].

Збір інформації щодо здійснення кіберзлочинності в країні повинні забезпечувати органи статистики, але, на жаль, вони поки ще не дають змоги одержати достовірні й чіткі дані щодо криміналістичної характеристики злочинів, які вчинюються у сфері використання комп'ютерних технологій в Україні, їх динаміки та структури. Це відбувається як через недосконалість праці статистики, так і через високу латентність цих видів злочинів, які підтверджуються дослідженнями інших вітчизняних дослідників.

Збір показників за видами кіберзлочинності в нашій країні відбувається, але за такими видами, як [11]:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
– несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;
– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється.

Цей перелік використовують і зараз при зборі інформації щодо кількості вчинених злочинів, пов'язаних з комп'ютерною технікою, але він застарілий і не дає можливості дослідити інші види цих злочинів, час іде, і класифікація оновлюється, з'являються нові види злочинів. Разом з цим статистика отримує дані не з першоджерел, а зі звітів правоохоронних органів України, що, в свою чергу, не дає картини щодо їхньої загальної кількості, адже ведуться підрахунки тільки злочинів, які входять до статей Кримінального кодексу України.

Для збору інформації щодо здійснення кіберзлочинів у країні доцільно використовувати метод анкетування, в якому автор запропонував розробити анкету, де буде внесена категорія "домогосподарства", яка рідко звертається до правоохоронних органів по допомогу в розкритті такого виду злочину. При розробленні анкети автор пропонує розподілити комп'ютерні злочини на такі групи [12]:

– злочини проти конституційних прав і свободи людини і громадянина;
– злочини проти життя і здоров'я;
– злочини проти честі й гідності особи;
– злочини проти власності;
– злочини у сфері комп'ютерної інформації;
– злочини проти суспільної моральності;
– злочини проти безпеки держави.

Питання щодо злочинів проти власності повинні містити такі запитання: чи доводилось вам стикатись з розкраданням ваших електронних коштів, якщо так, то як часто; чи стикались ви з тим, що, замовивши товар через мережу Інтернет, перерахувавши при цьому гроші, не отримали бажаного товару; чи доводилось вам перераховувати гроші через мережу Інтернет, при цьому вони не приходили в призначене місце, а з рахунку були зняті, якщо так, то як часто. До інформації щодо злочинів у сфері комп'ютерної інформації, насамперед, треба розробити запитання, які б показували розповсюдження спамів, зламування сайтів для своїх цілей та розповсюдження дитячої порнографії. Насамперед, за допомогою вказаної анкети можна буде відстежувати злочини, вчинені не тільки на підприємстві, а й у різних категоріях

домогосподарства. Анкетування щодо кількості злочинів можна проводити щорічно, використовуючи статистичну вибірку за розподілом фінансових доходів населення, при цьому виокремлювати різні групи. Проведення вказаного анкетування надасть можливість отримувати достовірні дані за всіма видами кіберзлочинності, адже ігнорування такого виду злочину, як кіберзлочинність, може призвести до виникнення загрози не тільки для конкретної людини, домогосподарства, приватних і державних структур, а й для національної безпеки окремих держав.

IV. Висновки

З проведеного дослідження класифікації кіберзлочинності можна дійти висновків, що чіткого розподілу вказаного виду злочинності ще не встановлено, його насамперед поділяють на злочини, пов'язані з порушенням конфіденційності, цілісності та доступності комп'ютерних даних і систем, та на злочини, які пов'язані або вчинені за допомогою комп'ютера. Автором вперше проведено дослідження існуючих засобів і методів збору інформації про кількість вчинених кіберзлочинів у країні та виявлено, що існуюча система збору даних поширюється лише на підприємства, а домогосподарства залишаються поза системою, разом з цим використовується застаріла класифікація цього виду злочину. Тому автором було запропоновано розробити анкету, в якій буде приведена чітка класифікація кіберзлочинності і яка буде поширюватися й на домогосподарства. Розробка та впровадження цього анкетування дасть змогу сприяти точному отриманню даних щодо вчинення комп'ютерних злочинів серед населення, що приведе до більш повного оцінювання рівня розвитку інформаційного суспільства в країні.

Список використаної літератури

1. Криміналістика : підручник [Електронний ресурс] / за ред. П.Д. Біленчука. – 2-ге вид., випр. і доп. – К. : Атіка, 2001. – 544 с. – Режим доступу: http://vse-znaniya.com/kriminalistika/klasifikatsiya-kompyuternih-zlochintsiv.html. – Назва з екрану.
2. Волобуєв А.Ф. Проблеми розслідування "комп'ютерних" злочинів / А.Ф. Волобуєв // Вестник Университета внутренних дел. – 1996. – № 1. – С. 63–70.
3. Пашнєв Д.В. Криміналістична класифікація комп'ютерних злочинів [Електронний ресурс] / Д.В. Пашнєв. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/Kyuv/2008_3/3-4/10.pdf. – Назва з екрану.
4. Соціальна Наукова Мережа. Кіберзлочинність в Україні [Електронний ресурс]. – Режим доступу: http://www.science-community.org/ru/node/16132. – Назва з екрану.
5. Інформаційне агентство УНІАН [Електронний ресурс]. – Режим доступу: http://economics.unian.net. – Назва з екрану.
6. Гуцалюк М.В. Впровадження ID-web як необхідна умова безпеки в Інтернет [Електронний ресурс] / М.В. Гуцалюк. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/bozk/18text/g18_30.htm. – Назва з екрану.
7. Українська справа. Як кіберзлочинці виманюють гроші українців [Електронний ресурс]. – Режим доступу: http://www.ukr-sprava.te.ua/korusno/31-yak-kiberzlochyntsi-vymaniuiut-hroshi-ukraintsiv. – Назва з екрану.
8. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби [Електронний ресурс] / Н.В. Савчук. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/tppe/2009_19/Zb19_48.pdf. – Назва з екрану.
9. Elcomrevue – основы электронной коммерции. Понятие киберпреступности [Электронный ресурс]. – Режим доступа: http://elcomrevue.ru/kibeoprestupnost-chto-eto/. – Название с экрана.
10. Марунченко О.П. Кіберзлочинність як загроза для безпеки для сучасної держави [Електронний ресурс] / О.П. Марунченко. – Режим доступа: http://archive.nbuv.gov.ua/portal/natural/Vsntu/polit/2012_136/2012_136/136_42.pdf. – Назва з екрану.
11. Злочинність в Україні : стат. зб. / Державна служба статистики України. – К., 2011. – 117 с.
12. Дзюндзюк В.Б. Поява і розвиток кіберзлочинності [Електронний ресурс] / В.Б. Дзюндзюк, Б.В. Дзюндзюк. – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf. – Назва з екрану.

Стаття надійшла до редакції 13.02.2014.

Дворник М.А. Статистические методы оценивания уровня киберпреступности на основе опроса домохозяйств

В статье осуществлена классификация киберпреступности, которая, в первую очередь, делится на преступления, связанные с компьютерными данными или системой, и преступления, совершаемые с помощью компьютерной техники. Исследованы методы сбора информации по осуществлению указанных преступлений по видам, распространяющиеся не на всех субъектов экономической деятельности. Предложено разработать анкету по всем видам киберпреступности, которая в частности будет распространяться на домохозяйства.

Ключевые слова: *киберпреступность, информационное общество, анкетирование, Интернет, компьютерная техника, методы оценки.*

Dvornik M. Statistical the methods for evaluating of the cybercrime level from household surveys

Relevance of the chosen theme of the article is based on that, during the development of the information society there are more possibilities for using computer technology and the Internet, but with this such kind of crime as cybercrime, is developedwhich in turn creates a major economic problem businesses, households and the economic development of the country as a whole.

All the important features of modern society, somehow related to computers, computer networks and computer data. The popularity of the Internet is not accidental, since it provides non-stop access to a wealth of information, fast data transfer, the ability for banking, shopping, stock transactions, transfer funds and more. However, with the widespread use of Internet technologies and increases in proportion to the threat of crime aimed at hackers, theft of personal information, blocking of information services, blackmail, fraud and so on.

From the article author's carried out research of classification of cybercrime, we can say that a clear division of the specified type of crime has not yet been established, it is primarily divided into offenses related to infringements of privacy, wholeness and availability of computer data and systems, and crimes which are connected or committed through computer. At the same time the author of the article the methods of gathering information on the implementation of the mentioned crimes by type, unfortunately nowadays are outdated and do not apply to all economic agents. On this basis, the author proposed to develop a questionnaire based on a more precise classification of cybercrime, which in particular will be distributed to households.

Gathering information about the implementation of cyber crime in the country, should be provided by the statistics, but unfortunately, they still do not allow to obtain reliable and accurate data on criminological characteristics of crimes that occur in the use of computer technology in Ukraine, their dynamics and structure. This is both due to the imperfection of labor statistics, and because of the high latency of such crimes, which are confirmed by other studies of local researchers. The technique of gathering information on the number of offenses committed in the households of the country, will help to see how many people are protected from these crimes.

Key words: *cybercrime, information society, questionnaire, Internet, computers, methods of evaluation.*