УДК 343.9:343.004.05:343.988

КІБЕРЗЛОЧИННІСТЬ: СУЧАСНИЙ СТАН ТА ОСОБЛИВОСТІ ВІКТИМОЛОГІЧНОЇ ПРОФІЛАКТИКИ

CYBERCRIME: CURRENT STATUS AND FEATURES OF VITICOMOLOGICAL PREVENTION

Фоменко О.В.,
студентка V курсу
Інститут прокуратури та кримінальної юстиції
Національного юридичного університету імені Ярослава Мудрого

Стаття присвячена висвітленню феномену кіберзлочинності, аналізу основних причин її поширення та віктимізації в цьому виді злочину. Проаналізовані статистичні дані та описана відповідна характеристика жертви кіберзлочину, наведений комплекс заходів віктимологічної профілактики, необхідних для усунення факторів віктимності користувачів комп'ютерних мереж.
Ключові слова: кіберзлочин, віктимність, жертва злочину, віктимологічна профілактика.

В статье рассматривается феномен киберпреступности, приведен анализ основных причин её распространения и виктимизации в этом виде преступления. Проанализированы статистические данные и описана соответствующая характеристика жертвы киберпреступления, сформулирован комплекс мер виктимологической профилактики, необходимой для устранения факторов виктимности пользователей компьютерных сетей.
Ключевые слова: киберпреступление, виктимность, жертва преступления, виктимологическая профилактика.

The article deals with the phenomenon of cybercrime. The author analyzes the relevance of the study of cybercrime and the main reasons for its dissemination. It is noted that with the increase of users of the computer network there is a tendency to increase the criminal encroachment of cybercriminals. Then there is a concept of a cybercrime in the text, which the author understands as such a socially dangerous act, committed in the virtual space and one way or another connected with the computer system. Based on this definition, signs of this type of crime are highlighted, and then the classification of types of cybercrime is given. Considering statistics on the distribution of cybercrime and victims of them, information is analyzed from both domestic sources and from other countries (United Kingdom, USA). Summing up the data, the author makes a short report on the typology of the victim of cybercriminals. He emphasizes that it is because of the great victimity of users that it is very necessary to develop measures to prevent cybercrime. The complex of state and community measures aimed at preventing crimes and reducing the risk of becoming victims of criminal offenses among the population and individual citizens is the main task of victimological prevention. The author makes a major accent on this statement in his article. In the final part, it has formed the security measures that each user of computer networks must adhere to.
Key words: cybercrime, victimity, victim of crime, victimological prevention.

Із стрімким розвитком технологій людство у кінці минулого століття вступило в еру комп'ютерів, і тепер майже кожний у своєму повсякденному житті мусить використовувати обчислювальні машини для полегшення життя. Інформаційні технології активно ширяться світом, і вже сьогодні жоден технологічний процес, фінансова операція або передача даних неможливі без комп'ютерних мереж. Масове включення електронно-обчислювальних машин до всіх сфер діяльності суттєво полегшили життя, водночас воно несе в собі безліч проблем. Перекладаючи частину своїх обов'язків на машину, людина не завжди розуміє ступінь ризику та відповідальності, що виникають у зв'язку з цим.

Як показує історичний досвід, будь-які зміни в суспільстві викликають і зміни в криміногенній ситуації. Комп'ютерізація не стала виключенням, і сьогодні у світовому інформаційному просторі часто зустрічається таке явище як кіберзлочинність.

Інтернет як доступний засіб комунікації та джерело інформації став притулком для сотні мільйонів користувачів, число яких збільшується щодня. Звісно, це викликає підвищений інтерес у кримінальних елементів суспільства. Внаслідок необізнаності та необачливості користувачів, вони автоматично стають мішенню для злочинних посягань з боку кіберзлочинців. Як наслідок, Інтернет-мережа стає інструментом для поширення вірусних програм, що посягають на безпеку особистих даних та прав інтелектуальної власності, а також полегшує доступ до порнографії, пошуку наркотиків, зброї тощо.

Якщо подивитись на результати дослідження Американського Центру стратегічних і міжнародних досліджень та компанії McAfee, проведених у 2013., то щорічні втрати світової економіки від кіберзлочинів досягли вже 500 мільярдів доларів. Це доказує актуальність наукового дослідження проблеми кіберзлочинності, що продовжує динамічно ширитися світом.

Метою статті є дослідження феномену кіберзлочинності, аналіз основних причин її поширення та віктимізації в цьому виді злочину, а також формулювання комплексу заходів віктимологічної профілактики, необхідних для усунення факторів віктимності користувачів комп'ютерних мереж.

Для цієї категорії злочинів є кілька назв: кіберзлочини, комп'ютерні злочини, злочини у сфері комп'ютерних технологій, злочини в сфері комп'ютерної інформації [3, с. 1]. Поняття «кіберзлочин» є відносно молодим для науки кримінального права, та складається зі слів «кібер» (розуміється як «кіберпростір», «віртуальний світ», «інформаційний простір») і «злочин». Тобто під поняттям кіберзлочину розуміють таке суспільно-небезпечне діяння, яке вчиняється у віртуальному просторі й так чи інакше пов'язане з комп'ютерною системою. С. Бренер виділила такі ознаки кіберзлочину: він найчастіше вчиняється на відстані із жертвою; суспільно-небезпечне діяння кіберзлочину часто є «автоматизованим», тобто воно виконується за допомогою комп'ютерних технологій і протягом короткого періоду часу, що прискорює швидкість скоєння, а, відповідно, і кількість; «автоматизація» кіберзлочину дозволяє їм вчинятися у будь-якому місці і у будь-який час незалежно від зовнішніх факторів; кіберзлочин є новим феноменом, і наука ще не здатна встановлювати моделі їх розповсюдження географічно та демографічно, як це робиться для інших злочинів [2, с. 435].

Окрім цього, виникають суто правові питання із визначенням місця вчинення кіберзлочину та відповідної юрисдикції, адже нерідко суб'єкт і жертва цього злочину знаходяться на великій відстані, і навіть у різних країнах.

Відповідно до статистичних даних Генеральної прокуратури України, кількість зареєстрованих в розрізі регіонів України упродовж 2016 р. злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

(ст. ст. 361–363-1 КК України) сягнула 1018, з яких справи за 501 злочином було направлено до суду. А за перше півріччя 2017 р. в Україні кількість кіберзлочинів, що потрапили у поле зору поліцейських, становить 705. При цьому слід враховувати, що до цих статистичних даних враховуються тільки частина з тих діянь, які відносять до кіберзлочинів.

Але глобально можливість переслідування кіберзлочинності має безліч складнощів. По-перше, це властива даному виду злочинів латентність, що спотворює статистичний облік і не дає побачити реальну картину. По-друге, в нашій країні взагалі відсутній відокремлений статистичний облік злочинів, віднесених до категорії кіберзлочинів. Разом з тим, наявні статистичні показники не враховують деякі «традиційні» злочини, вчинені з використанням автоматизованих технологій.

У літературі зустрічаються різні класифікації кіберзлочинів. В залежності від об'єкта, на який вони посягають, виділяють такі:

– кіберзлочини, що завдають шкоди конкретним об'єктам (порушення роботи банківської системи, викрадення конфіденційної інформації з особистого комп'ютера потерпілого);

– кіберзлочини, які посягають на невизначене коло об'єктів (розповсюдження комп'ютерних вірусів).

За природою злочину виділяють:

– кіберзлочини, що є традиційними злочинами, але вчиняються за допомогою комп'ютерних технологій та Інтернету (порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками тощо);

– кіберзлочини, що стали можливі завдяки новітнім комп'ютерним технологіям (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку).

Сьогодні представники кіберполіції до основних видів кіберзлочинності відносять:

– шахрайство з пластиковими платіжними картками;

– фальшиві Інтернет-аукціони, а також махінації, що відбуваються в сфері купівлі-продажу товарів і послуг через безкоштовні дошки оголошень у віртуальному просторі;

– викуп і реєстрація доменних імен (киберсквоттінг);

– крадіжка послуг (фоункрейкінг);

– створення вірусів;

– крадіжка інформації та особистих даних.

За даними ООН, найпоширенішим злочином з використанням інформаційних технологій в світі є крадіжка інформації при проведенні фінансових операцій через Інтернет (наприклад, дані кредитних карт або банківських рахунків).

Типологія поширення даного типу злочинів досить проста, і жертвою на сьогодні може стати кожний активний користувач всесвітньої мережі. Департамент кіберполіції зазначає, що найбільше проблем сьогодні виникає через Інтернет-магазини. Явище електронної комерції зростає щодня, так само зростає і грошовий обіг в мережі Інтернет, а тому відповідно збільшується кількість Інтернет-шахраїв. Злочинці швидко пристосовуються до нових технологій і активно використовують їх для реалізації схем по заволодінню коштами простих громадян. Водночас вражає різноманітність цих схем: від використання масштабних Інтернет-аукціонів і торгових платформ до створення фейкових сторінок або груп з продажу неіснуючих товарів.

Також істотний вплив на поширеність кіберзлочинів справляє такий соціально-психологічний чинник, як відсутність прямих контактів та взаємозв'язків між злочинцем та потерпілим, а також між злочинцем та предметом злочину. Ці зв'язки опосередковуються наявністю додаткового елемента – технологічних пристроїв, що неначе «знеособлює» кіберзлочинця.

Дистанційна віддаленість і «віртуалізація» збитку, що заподіюється у кіберпросторі, обумовлює його специфічне уявлення жертвою злочину. Потерпіла особа, яка виявляє заподіяний їй збиток, не здатна в повній мірі усвідомити характер і ступінь суспільної небезпеки вчиненого щодо неї діяння. Таким чином, у більшості випадків жертва сприймає скоєний проти неї кіберзлочин і заподіяну ним шкоду як абстрактне «зло», яке не має перспективи бути відшкодованим.

Що стосується юридичних осіб як жертв кіберзлочинності, то цікавим є факт, що достатньо велика кількість підприємств дотримується думки про рівнозначність втрат від кібератак з витратами, які є необхідними для впровадження системи безпеки. Тобто власники юридичних фірм впевнені у відсутності потреби піклуватися про безпеку власних технічних пристроїв та інформаційних ресурсів.

Проте не всі знають, що втрата фінансових активів або конфіденційної інформації не вичерпують весь перелік збитків від шкідливих дій в кіберпросторі [1, с. 102]. На додаток, наслідками незаконної кібердіяльності є збитки, які наносяться репутації компанії або особистості, а також альтернативні витрати, необхідні для усунення збоїв в системі обслуговування клієнтів.

Існують різні погляди на те, хто найчастіше стає жертвою кіберзлочинності, і чи можливо взагалі передбачити ймовірну групу ризику. На думку В. Хахановського, потерпілими від кіберзлочинів найчастіше є юридичні особи [4, с. 221]. Це пояснюється тим, що процес комп'ютеризації широко охоплює, перш за все, юридичних осіб (організації, установи). Ґрунтуючись на такій точці зору, існує статистика, відповідно до якої на першому місці серед потерпілих від кіберзлочинів осіб є власники комп'ютерної системи (79%); за ними йдуть клієнти, що користуються їх послугами (13%), та інші особи (8%) [1, с. 194]. Але ми вважаємо, що більш правильною є точка зору про те, що найбільше від кіберзлочинності страждає молодь, яка досить часто користується соціальними мережами та публічними мережами WI-FI. При цьому вони не турбуються навіть про такі заходи безпеки, як встановлення пароля або антивірусного програмного забезпечення. Опитування показали, що масштаб кіберзлочинності у споживчому секторі сягнув 1 млн. жертв на день.

При цьому потерпіла сторона неохоче повідомляє про це правоохоронним органам. Це пояснюється наявною недовірою до правоохоронних органів, їх некомпетентністю, а також через острах можливого виявлення власних незаконних дій потерпілого тощо. Така ситуація створює високий рівень латентності кіберзлочинів.

У зв'язку з неповнотою вітчизняних статистичних даних для встановлення повної віктимологічної характеристики жертв кіберзлочинів необхідно звернутися до зарубіжних досліджень. Так, за даними Національного бюро боротьби із шахрайством у Великобританії, сформовано такі основні характеристики жертви кіберзлочину:

− на частку фізичних осіб припадає 85% всіх кіберзлочинів, тоді як на юридичних осіб всього 13%;

− близько 24% жертв кіберзлочинності були визначені як потенційно вразливі (тобто такі, що стають або можуть стати жертвами повторно);

− жертвами схильні бути особи, віком від 15 до 49 років;

− чоловіки схильні втрачати від кіберзлочинності в 3 рази більше, ніж жінки;

− збиток від крадіжки інтелектуальної власності та конфіденційної ділової інформації є найбільш важливою категорією збитку;

− жінки у 6 разів частіше стають жертвами шахрайства від «Інтернет-магазинів», ніж чоловіки [6, с. 3].

Виходячи з цього, можна зробити висновок, що жертвою кіберзлочину може стати будь-яка особа, проте на індивідуальному рівні можна виділити такі типи жертв кіберзлочинів:

– випадкова жертва – коли особа стає такою внаслідок збігу обставин;

– жертва з незначним ступенем ризику – віктимність виникла під впливом конкретної несприятливої ситуації;

– жертва з підвищеним ступенем ризику;

– жертва з високим ступенем ризику – особа, морально-соціальна деформація якої не відрізняється від правопорушників [4, с. 242].

Вже зараз необхідність запобігання кіберзлочинам є дуже актуальною через віктимність користувачів. Фактори, що сприяють поширенню кіберзлочинності та віктимізації її жертв, пов'язані з недоліками соціального контролю: ігнорування користувачами вимог про дотримання інформаційної безпеки, низька компетентність правоохоронних органів у боротьбі з кіберзлочинністю та неналежна їх технічна оснащеність.

Тому на сьогодні виявлення, усунення та нейтралізація факторів, які формують віктимну поведінку та зумовлюють вчинення кіберзлочинів є нагальним питанням. Здійснення комплексу державних та громадських заходів, що орієнтовані на запобігання злочинам та зниження у населення та окремих громадян ризику стати жертвами злочинних посягань, є головним завданням віктимологічної профілактики. Основними напрямами її дії є формування та розповсюдження рекомендацій серед користувачів комп'ютерних технологій та мережею Інтернет. Зокрема, щоб не стати жертвою даного виду злочину, вироблені такі рекомендації:

1. У разі здійснення Інтернет-покупки:

– варто переконатися у надійності магазину або продавця. Для цього можна зв'язатися з представником Інтернет-магазину або безпосередньо з продавцем. Також в Інтернеті слід перевірити магазин за назвою або за номером телефону продавця з метою виявлення відгуків його клієнтів;

– необхідно перевірити вартість товару, який ви бажаєте придбати. Якщо його ціна набагато нижча за інші Інтернет-магазини, то слід бути обачними;

– користувачам варто звертати увагу на вимогу про проведення передоплати. Правило про обов'язковість попередньої оплати повинно насторожувати, а відтак, виконувати цю вимогу можна лише з перевіреними та надійними суб'єктами.

2. Користуючись тим чи іншим Інтернет-ресурсом, слід дотримуватись елементарних правил, які встановлені для користувачів:

– після завершення роботи з комп'ютером – виключайте його;

– не потрібно відкривати електронні повідомлення від невідомих відправників;

– регулярно оновлюйте антивірусну програму для захисту комп'ютера;

– ніколи не розголошуйте свій пароль і часто міняйте його.

3. Ніколи не можна розголошувати конфіденційну інформацію про себе в мережі Інтернет, а також повідомляти її на будь-яких електронних ресурсах. Також не залишайте свої банківські або фінансові дані за запитом сайту під виглядом безпеки.

4. Для захисту від фейкових та фішингових сайтів слід звертати увагу на такі візуальні елементи сайту, як назва протоколу, домену тощо.

5. Безпечно користуватися лише ліцензованими програмами.

Особливі правила безпеки вироблені для користувачів банківської платіжної системи. Серед них такі:

– ніколи не можна повідомляти персональну інформацію та інформацію щодо платіжної картки на вимогу нібито банківського працівника (якщо вам на мобільний поступив подібний дзвінок тощо);

– не рекомендується постійно зберігати всі грошові кошти на банківській платіжній картці. Також доречно буде встановити ліміт на щоденне або разове зняття грошових коштів;

– перед початком роботи з банкоматом необхідно уважно його оглянути на предмет додаткових встановлених злочинцями девайсів (камера, додаткова клавіатура тощо) [5, с. 241].

Юридичним особам як особливій категорії потерпілих від цієї категорії злочину органи правопорядку наполегливо радять враховувати кібербезпеку як невід'ємну складову бізнесу, аби захистити свою справу від посягань з боку кіберзлочинців.

Як **висновок**, є важливим, щоб всі учасники Інтернет-мережі мали елементарну поінформованість та прислухалися до вищезазначених правил безпеки, аби не потрапити у неприємну ситуацію. У разі, якщо ви все ж таки стали жертвою кіберзлочину – негайно звертайтеся до поліції.

ЛІТЕРАТУРА

1. Абламський С. Є. Проблемні питання захисту прав потерпілого від кіберзлочинності / С. Є. Абламський // Актуальні питання розслідування кіберзлочинів : матеріали міжнародної науково-практичної конференції. – Х. : 2013. – С. 192–195.

2. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій / К. В. Юртаєва // Форум права. – 2009. – № 2. – С. 434–441.

3. Довбиш М. Кіберзлочинність в Україні / М. Довбиш // Scientific Social Community (Соціальна наукова мережа). – 2013 [Електронний ресурс]. – Режим доступу : https://www.science-community.org/ru/node/16132.

4. Кравцова М. А. Понятие киберпреступности и её признаки / М. А. Кравцова // Часопис Київського університету права. – 2015. – № 2. – С. 320–325.

5. Шагірманов Д. О. Деякі питання віктимологічного запобігання кіберзлочинності / Д. О. Шагірманов // Теорія і практика віктимології : матеріали Всеукраїнської конференції для студентів, аспірантів, ад'юнктів, здобувачів, присвяченої 50-річчю з дня заснування кафедри кримінології та кримінально-виконавчого права (м. Харків, 12 листопада 2015 року) / за ред. А. П. Гетьмана, Б. М. Головкіна. – Х. : Національний юридичний університет ім. Ярослава Мудрого, 2015. – С. 241–242.

6. Cyber Crime – Victimology Analysis : February 2016 / National Fraud Intelligence Burea // City of London Police – National Policing Lead For Fraud. – 2010 [Електронний ресурс]. – Режим доступу : https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf.