Горбенко А.В.,
студентка 6 курсу, 8 групи, Інституту прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого

ЯК СТАЮТЬ ЖЕРТВОЮ КІБЕРЗЛОЧИНІВ

*Ключові слова:*кіберзлочини, віктимність, жертва кіберзлочину, віктимологічна профілактика

Анотація. У тезах розглянуті комплекси заходів щодо віктимологічної профілактики.

*Аннотация.*В тезисах рассмотрены комплексымероприятий по поводу виктимологическойпрофілактики.

*Ключевые слова:*киберпреступления, виктимность, жертва киберпреступления, виктимологическаяпрофилактика

Keywords: cybercrime, victimization, victim of cybercrime, victimological prevention

Summary. The theses consider of measures on victimological prevention are considered in the abstracts.

На сучасному етапі розвитку Інтернет є не просто засобом комунікації між користувачами, але і, так званим, інструментом, який полегшує життя. Сучасна людина використовує мережу Інтернет практично в усіх серах життєдіяльності: фінансові операції, передача даних та інші процеси. Проте, виникають певні проблеми та загрози. В епоху суцільної комп'ютеризації складно відчувати себе захищеним, оскільки, як відомо, будь-які зміни у суспільстві тягнуть за собою зміни у криміногенній ситуації. Із розвитком новітніх технологій в інтернеті поширюється різного роду діяльність, особливого розвитку зазнала кіберзлочинність, яка активно процвітає. За сферою злочинних проявів особливе місце посідають злочини у сферах захисту інформації, використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку [8, с. 17].

Сьогодні в суспільстві відбуваються інтенсивні процеси інформатизації та інтелектуалізації, прискореними темпами формується інформаційне суспільство, особливістю якого є комп'ютеризація всіх сфер людського життя. Останнім часом комп'ютерні технології та комп'ютерні системи використовуються в більшості злочинів як засіб їх вчинення [5, с. 1297].Динаміка злочинності на протязі останніх років характеризується хвилеподібними коливаннями, які чітко показують виражену тенденцію до зростання злочинності на території нашої держави. Висока складність соціальних систем є безумовною ознакою нелінійності законів залежності станів таких систем від певних зовнішніх та внутрішніх факторів [7].

Кіберзлочинність (або ще по іншому називають злочинність в сфері інноваційних технологій, комп'ютерні злочини тощо) є історично обумовленим і мінливим явищем. Цей вид злочинності поряд з такими поняттями як економічна злочинність, організована злочинність, корупція, легалізація злочинних доходів хоча і з'явилось нещодавно, але міцно увійшло у понятійний апарат кримінологів і практичних працівників. Не так давно злочинам в кіберсфері на національному рівні приділялась незначна увага, вважалось, що кіберзлочинність може представляти реальну загрозу лише в далекому майбутньому, тепер майже ні в кого не виникає

сумнівів, що частка кіберзлочинності в структурі злочинності України значно збільшилася [1, 81].

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 в 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, 435]. З точки зору філософії, парні категорії «хаос» і «порядок» взаємопов'язані, співвідносяться як діалектичні протилежності, постійно переходять одна в іншу. Проте у впорядкованих явищ є причина, що їх породжує, визначає повторюваність, послідовність і прогнозованість розвитку [6, 204].

У науковій літературі побутують різні думки про те, хто ж може стати жертвою кіберзлочинності ,і чи можливо взагалі виокремити та передбачити таку групу ризику. Як зазначав В. Хохановський: потерпілими від кіберзлочинів найчастіше є юридичні особи[3, 221]. Проте, на нашу думку, у сучасному світі найчастіше від кіберзлочинів страждає молодь, оскільки саме вона активно використовує WI-FI та користуєтьсясоціальними мережами. При цьому, важливо звернути увагу на те, що зазвичай при здійсненні своїх дій, молодь нехтує елементарними заходами безпеки, наприклад, дотримання вимог інформаційної безпеки, встановлення різноманітних паролів, до того ж відмінних один від одного, ненадання своїх паролів, номерів карток невідомий або сумнівним особам, або ж встановлення антивірусного програмного забезпечення. Практика показує, що з кожним днем масштаб кіберзлочинності невпинно зростає, при цьому потерпілі особи рідко повідомляють про неправомірні дії щодо себе. Це свідчить про те, що кіберзлочинність має високу латентність.

Кожен із нас може стати жертвою кіберзлочинів через власну віктимність. Б.М. Головкін зазначає, за різнихобставин жертвами злочинівможуть стати будь-які особи, незалежно від статі, віку, національності, соціального становища, рівня доходів, місця

проживання. Між тим практика показує неоднаковий рівень уразливості людей перед злочинними посяганнями. Це пов'язано не тільки з соціально-демографічними відмінностями населення, але й з несприятливими середовищними умовами проживання та небезпечною поведінкою за конкретних обставин[4, 162].

Для профілактики віктимологічної поведінки варто розробити і постійно оновлювати комплекс державних та громадських заходів, які орієнтовані не тільки на запобігання, але і на зниження ризиків стати жертвами кіберзлочинів. Це може досягатися формуванням і розповсюдженням простих та коротких рекомендацій серед користувачів мережі Інтернет, наприклад, через соціальні мережі. Завдяки цьому, також буде підвищуватися рівень правосвідомості як в цілому населення, так і окремих груп та категорій громадян.

Аналізуючи практику, можна сформувати такі рекомендації, щоб не стати жертвою кіберзлочинів:

У разі здійснення інтернет-покупок необхідно:

переконатися в надійності інтернет-магазину, продавця чи сторінки (зв'язатися з представником, елементарно зателефонувавши за номером телефону. Відсутність контактних телефонних номерів може бути першим свідченням щодо ненадійності. Також варто перевіряти наявність відгуків, окрім тих, які наявні на сторінці представника);

перевірити вартість товару(ціна товару, який Ви бажаєте придбати не може бути набагато нижчим ніж у інших інтернет-магазинах, сайтах і т.д.).

Сьогодні, важливо звертати також увагу на спосіб оплати покупки, оскільки безліч шахраїв користуються довірливістю покупців та вимагають проведення передоплати. Якщо продавець настійливо вимагає здійснювати передоплату це має істотно насторожувати. Тому проводити такі дій варто лише з ретельно перевіреними суб'єктами.

Варто також дотримуватися елементарних правил для користувачів:

- виключати комп'ютер після завершення роботи з ним;

- не розголошувати свої паролі та періодично їх змінювати, це певною мірою зможе захистити Вашу інформацію від сторонніх;

- оновлювати антивірусні програми з метою захисту комп'ютера;

- при використанні електронної пошти звертати увагу на листи, надіслані від невідомих користувачів та такі, що віднесені до папки «Спам».

Молодь часто не зважає на те, яку інформацію розголошує в мережі, тож важливо не розголошувати конфіденційну інформацію про себе та не повідомляти її на будь-яких електронних ресурсах. Тож завжди необхідно зважати на те, які дані потребує сайт для входу.

Реалії сьогодення практично змушують нас використовувати банківські платіжні картки. Їх використання потребує особливих правил безпеки:

- не повідомляти жодної інформації щодо платіжної картки третім особам, особливо обережним варто бути із, так званими, представниками банків;

- не давати свою картку у користування іншій особі;

- не переписувати і тим паче не зберігати дані платіжної картки на паперових чи електронних носіях;

- постійно перевіряти рух коштів на рахунку та ін.

Отже, важливо постійно інформувати користувачів мережі Інтернет щодо стану кіберзлочинності задля профілактики віктимологічної поведінки. Розробляти та оновлювати заходи, орієнтовані на запобігання та зниження ризиків стати жертвою кіберзлочинів.

ЛІТЕРАТУРА:

1. Таволжанський О. В. Кримінологічні аспекти кіберзлочинності у сучасних умовах / О. В. Таволжанський // TheJournalofEasternEuropeanLaw = Журнал східноєвропейського права. – 2016. – № 31. – С. 80–86. Режим доступу: http://dspace.nlu.edu.ua/bitstream/123456789/17724/1/Tavolzhanskyi_80-86.pdf

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

3. Кравцова М.А. Понятиекиберпреступности и ее признаки / М.А. Кравцова // Часопис Київського університету права. – 2015. - № 2. – с. 320-325

4. Головкін Б. М. Як стають жертвами злочинів // Проблеми законності. Вип. 136. 2017. С. 161 – 172. URL: http://nbuv.gov.ua/UJRN/Pz_2017_136_19

5. Ovcharenko, Mykola O; Tavolzhanskyi, Oleksii V; Radchenko, Tetiana M; Kulyk, Kateryna D; Smetanina, Nataliia / CombatingIllegalDrugsTraffickingUsingtheInternetbyMeansoftheProfilingMethod / Tavolzhansky O. V.// V.JournalofAdvancedResearchinLawandEconomics; Craiova Том 11, Изд. 4(50), (Summer 2020): 1296-1304.

6. Таволжанський О. В. Сучаснірealіїкіберпростору України / О. В. Таволжанський // Забезпеченняправопорядку в умовахкоронакризи :матеріалипанельноїдискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24 верес. 2020 р. – Харків, 2020. – С 203–208.

7. Robotization of manufacturing process: economic and social problems and legal ways of their solution / O. E. Kostyuchenko, T. V. Kolesnik, Z. V. Bilous, O. V. Tavolzhanskyi // Financial and credit activity: problems of theory and practice. – 2019. – Vol. 3, is. 30. – P. 454–462.

8. Головкін Б. М. Види злочинності // Журнал Східноєвропейського права. 2015. № 18. С. 14-21.URL: http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf

Науковийкерівник к.ю.н., доц.О.В. Таволжанський