УДК 004.946.5.056

Софія Михайлівна Сапужак,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: характеристика поняття та способи захисту

Стрімкий розвиток інформаційних технологій, інформатизація та комп'ютеризація, створення глобального інформаційного простору сформували принципово нові субстанції – інформаційне суспільство, інформаційний і кібернетичний простори, які мають невичерпний потенціал і відіграють провідну роль в економічному та соціальному розвитку країн світу. Однак, створення інформаційного суспільства може призвести і до виникнення багатьох інформаційних загроз. Повною мірою ми всі змогли це відчути 27 червня 2017 року, у день, який став «чорним вівторком» для кібербезпеки нашої країни. Протягом одного дня комп'ютерний вірус «Ransom:Win32/Petya» атакував приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережні супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади та місцевого самоврядування тощо.

Вважаємо, що обрана тема є надзвичайно актуальною, оскільки вітчизняні реалії та кримінальна статистика свідчать про недостатню обізнаність пересічних громадян про кіберзлочинність та способи захисту від неї.

Теоретичною базою, послужили наукові публікації В. Гібсона, М. Камчатного, О. Манжая, Л. Бурячка, Б. Толубка, В. Хорошка, С. Гнатюка.

Метою даної роботи є дослідження феномену кіберзлочинності, аналіз основних її проявів, а також формулювання комплексу заходів, щодо захисту громадян від даних злочинних діянь.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», поняття кіберзлочин (комп'ютерний злочин) трактується, як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом

© Сапужак С.М., 2019

України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Нині чинним Кримінальним кодексом України передбачено кримінальну відповідальність за:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2);

4) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363);

6) перешкоджання роботі електронно-обчислювальних машин комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) [2].

За даними ООН, найпоширенішим кіберзлочином у 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 Інтер-

нет-аукціонів і торгових платформ до створення фейкових сторінок або груп з продажу неіснуючих товарів [3, с. 44–45].

І все ж є певний набір заходів, який мінімізує ризики, як для звичайних людей, як і для співробітників компаній, які хочуть захистити себе від різних кіберзагроз та кібезлочинів, а саме:

- дотримання «цифровий гігієни»: грамотно працювати з електронною поштою, не відкривати підозрілі вкладення, не переходити по посиланнях з листів з незнайомих джерел, не завантажувати неліцензійні файли, які можуть містити віруси, постійно оновлювати ліцензійне програмне забезпечення як на персональних комп'ютерах, так і на інших гаджетах, до приклади смартфони, планшети;

- ділитися своїми персональними даними тільки після того, як зможете переконатись, що будь-яка компанія або навіть держпідприємство, якому ви пересилаєте свої дані, дійсно несе за них відповідальність, вживає всіх заходів для їх збереження;

- не 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;

- всі важливі дані повинні мати резервні копії. Рекомендовано зберігати особливо цінні дані в сховищах, які не підключені до інтернету.

Отже, здавалося б такі елементарні правила, але як же ж важливо, щоб всі учасники Інтернет-мережі були ознайомлені та прислухалися до них, аби не потрапити у неприємну ситуацію. У разі, якщо ви все ж таки стали жертвою кіберзлочину – негайно звертайтеся до поліції.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.
3. Кравцова М. О. Запобігання кіберзлочинності в Україні : монографія / за заг. ред. О. М. Литвинова. Харків : Панов, 2016. 212 с.

Одержано 01.11.2019