3. Кримінальний процесуальний кодекс в редакції від 19.04.2024 року № 4651-VI URL: https://zakon.rada.gov.ua/ laws/show/4651-17#Text (дата звернення 28.04.2024).

4. Правила адвокатської етики в редакції від 15.02.2019 року № n0001891-17 URL: https://zakon.rada.gov.ua/ rada/show/n0001891-17#Text (дата звернення 28.04.2024).

5. Про адвокатуру та адвокатську діяльність: Закон України в редакції від 03.08.2023 № 5076-VI URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text (дата звернення: 28.04.2024).

Лисенко Богдан Олександрович,
здобувач вищої освіти навчально-наукового інституту № 1 Національної академії внутрішніх справ
Науковий керівник:
Антонюк Поліна Євгеніївна
професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидат юридичних наук, доцент

СПОСОБИ ВЧИНЕННЯ ШАХРАЙСТВ ІЗ ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

З розвитком технологій та проникненням інтернету в усі сфери нашого життя шахраї все активніше використовують кіберпростір для своїх кримінально протиправних схем. Особливої гостроти це явище набуло з початком повномасштабного військового вторгнення на територію України, коли активізувалися більшість «темних» хакерів, метою діяльності яких, окрім заволодіння матеріальними цінностями, є також допомога ворогу, заволодіння інформацією користувачів та поширення провокацій, що в подальшому може призвести до деморалізації громадян та розсіювання паніки серед населення.

В кримінальному кодексі Україні передбачена відповідальність за кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку [1, розділ XVI].

В 2005 році Україна ратифікувала Конвенцію «Про кіберзлочинність», у ст. 8 якої шахрайство, пов’язане з комп’ютерами, розглядається як дії, що призводять до втрати майна іншої особи шляхом: a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, b. будь-якого втручання у функціонування комп’ютерної системи, - з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи [2].

Огляд вітчизняної та зарубіжної практики правоохоронних органів дозволяє виділити наступні найпоширеніші сучасні способи шахрайства з використанням кіберпростору:

1. Фішинг. Шахраї надсилають електронні листи або SMS-повідомлення, які виглядають так, ніби вони відправлені з легітимного джерела, наприклад, банку, онлайн-магазину або соціальної мережі. Ці повідомлення містять посилання або вкладення, які, якщо їх відкрити, можуть перевести користувача на «фейковий» сайт, що імітує легітимний. На цьому «фейковому» сайті користувача можуть попросити ввести свої персональні дані, такі як номер банківського рахунку, пароль або номер кредитної картки тощо. Після того, як шахраї отримають цю інформацію, вони можуть використовувати її для крадіжки коштів або вчинення інших кримінальних правопорушень.

2. Спішінг. Полягає в тому, що шахраї телефонують потенційним жертвам, представляючись співробітниками банку, служби підтримки клієнтів або інших авторитетних організацій. Вони можуть повідомити жертві про те, що її рахунок був скомпрометований або що їй необхідно негайно оновити свою персональну інформацію. Потім вони можуть попросити жертву ввести свої персональні дані або переказати їм гроші.

3. Онлайн-аукціони та оголошення. Шахраї розташовують «фейкові» оголошення про продаж товарів або послуг на онлайн-аукціонах або сайтах з оголошеннями. Коли потенційна жертва виявляє інтерес до оголошення, шахрай може попросити її зробити передоплату за товар або послугу, які насправді не існують. Після отримання передоплати шахрай зникає.

4. Соціальні мережі (SCAM). Зловмисники створюють «фейкові» профілі в соціальних мережах або захоплюють реальні профілі. Потім вони можуть використовувати ці профілі для того, щоб зв’язатися з друзями та підписниками жертви, прохаючи їх про допомогу або позику грошей. Шахраї також можуть використовувати «фейкові» профілі для поширення дезінформації або пропаганди.

5. Ransomware. Вимагачі використовують тиск як основну тактику, і, хоча існує багато підходів до програм-вимагачів, основна загроза, яку вони демонструють полягає в шифруванні важливих даних та унеможливленні доступу до них жертви. Потім вони вимагають викуп від декілька сотень до пару десятків тисяч доларів за «розшифровку» файлів. Якщо жертва не заплатить викуп, шахраї можуть видалити файли або продати їх на чорному ринку [3, с. 3].

6. Криптовалютні шахрайства. Шахраї пропонують потенційним жертвам інвестувати в криптовалюту, якої насправді не існує. Вони можуть обіцяти жертвам високу прибутковість від своїх інвестицій. Після того, як жертва інвестує свої гроші, шахраї зникають.

Це лише деякі з найпоширеніших способів вчинення шахрайства з використанням кіберпростору.

Щоб уберегти себе від кібершахрайства, слід дотримуватися певних порад щодо «кібергігієни»:

- не відкривати посилання або вкладення в електронних листах або SMS-повідомленнях від невідомих відправників;
- не вводити свої персональні дані на сайтах, в репутації яких ви не впевнені;
- бути обережними при онлайн-покупках, особливо якщо ви купуєте товари або послуги за занадто низькою ціною;
- не надавати персональну інформацію людям, які зв'язуються з вами в соціальних мережах, та не пересилати кошти незнайомцям.

Важливо пам'ятати, що кіберзлочинність постійно розвивається, і з'являються нові способи шахрайства. Тому слід бути пильними, знати про ризики та вживати заходів безпеки для захисту себе та своїх даних.

Список використаних джерел

1. Кримінальний процесуальний кодекс України від 13 квіт. 2012 р. № 4651-VI. URL : https://zakon.rada.gov.ua/ laws/show/4651-17#Text

2. Конвенція про кіберзлочинність (Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71). URL: https://zakon.rada.gov.ua/ laws/show/ 994_ 575#Text

3. Ransomware: a look at the criminal art of malicious code, pressure, and manipulation (2021).

Литвинюк Ілона Сергіївна,
здобувач вищої освіти навчально-наукового інституту № 1 Національної академії внутрішніх справ
Науковий керівник:
Патик Леся Леонідівна,
доцент кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидат юридичних наук, доцент

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ В УМОВАХ ВОЄННОГО СТАНУ

Сьогодні ми стикаємося з численними конфліктами, які виникли після введення воєнного стану. Зростає кримінальна активність, що може стати серйозною загрозою для мирного населення. Вже понад два роки ми перебуваємо у стані активної фази війни. У таких умовах питання протидії кримінальним правопорушенням важливе як ніколи.

Міжнародні організації, зокрема ООН та ЄС, відіграють значну роль у здійсненні контролю за правопорядком під час воєнного стану