Богула Софія Дмитрівна
Студентка н.гр. 302 СПС ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ПСИХОЛОГІЧНІ НАСЛІДКИ КІБЕРШАХРАЙСТВА

У сучасному світі, де більшість життєвих процесів відбуваються в онлайн-просторі, людина стає особливо вразливою до кіберзлочинів. Одним із найпоширеніших проявів кіберзлочинності є *кібершахрайство* – злочин, який не лише завдає матеріальної шкоди, а й має серйозні психологічні наслідки для жертв.

Кібершахрайство є різновидом кіберзлочинності, який полягає у використанні комп'ютерних технологій, мережі Інтернет або електронних комунікацій для незаконного заволодіння чужим майном, коштами чи персональними даними. Тобто, основною ознакою кібершахрайства є введення жертви в оману з використанням цифрових засобів. Це може бути створення фішингових сайтів, підроблених сторінок банків, онлайн-магазинів або соціальних акаунтів, через які шахраї отримують доступ до коштів чи особистої інформації.

До основних форм кібершахрайства належать:

1. Фішинг – отримання особистих даних користувача (логінів, паролів, реквізитів карток) шляхом підробки сайтів або електронних листів.
2. Онлайн-шахрайство в соціальних мережах – створення фейкових акаунтів для виманювання грошей чи даних.
3. Шахрайство з банківськими картками (скімеринг) – незаконне копіювання реквізитів картки та використання їх для крадіжки коштів.
4. Інвестиційне шахрайство – пропозиція «високоприбуткових» онлайн-вкладень, які насправді є фінансовими пірамідами.
5. Love scam – емоційне маніпулювання жертвами через знайомства онлайн з метою заволодіння їхніми фінансами.

Проблема кібершахрайства виходить далеко за межі матеріальних втрат. Вона має глибокі психологічні наслідки, які можуть впливати на емоційний стан, самооцінку, довіру та соціальну поведінку людини.

1. *Емоційний шок і гострий стрес*.

Жертви часто переживають сильне потрясіння після усвідомлення обману. З’являються почуття розгубленості, страху, сорому, гніву, а також соматичні прояви – безсоння, головний біль, прискорене серцебиття.

2. *Втрата довіри до людей і систем*.

Після пережитого шахрайства люди часто перестають довіряти не лише незнайомцям онлайн, а й знайомим, фінансовим установам, навіть власним родичам. Це може призводити до соціальної ізоляції.

3. *Почуття провини та сорому*.

Жертви часто звинувачують себе у «наївності» або «недалекоглядності», що формує почуття власної безпорадності. Особливо це характерно для молодих людей і літніх осіб, які не мають достатніх знань у сфері кібербезпеки.

4. *Розвиток тривожних і депресивних станів*.

Після шахрайства може розвинутися тривожний розлад, депресія, зниження самооцінки та навіть посттравматичний стресовий розлад (ПТСР). Люди часто уникають цифрових технологій, відчувають страх повторного обману.

5. *Порушення соціальних контактів*.

Після обману у сфері онлайн-знайомств (love scam) жертви можуть уникати нових стосунків, мають труднощі у встановленні емоційних зв’язків і довірі до партнерів.

Для ефективної протидії цьому явищу необхідна ***комплексна стратегія***, що поєднує:

1) Інформаційно-просвітницьку роботу (навчальні кампанії, тренінги з кібергігієни).

2) Психологічну підтримку жертв – створення гарячих ліній, безкоштовних консультацій.

3) Використовувати двохфакторну автентифікацію.

4) Підвищення кіберграмотності населення, особливо дітей, підлітків і людей похилого віку.

Таким чином, кібершахрайство – це не лише фінансова загроза, а й серйозна соціально-психологічна проблема. Воно підриває довіру між людьми, провокує тривожність і емоційні травми, особливо серед вразливих груп населення. Тому важливо розвивати не лише технічні засоби захисту, а й психологічні програми підтримки, спрямовані на відновлення внутрішньої безпеки та довіри користувачів цифрового середовища.

Список використаних джерел:

1. Кіберзлочинність та електронні докази: навчальний посібник // Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. // Львівський національний університет імені Івана Франка, 2022 р. // ст. 14–15 // URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

2. Кібербезпека: правові та психологічні аспекти // Пєтков В. В. // Київ: КНТ, 2021 р. // ст. 63–70 // URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf
3. Поради з кібербезпеки для громадян // Міністерство цифрової трансформації України // офіційний сайт // URL: https://thedigital.gov.ua/

Чистоклєтова Анна Денисівна
Студентка н.гр. 302 СПС ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

МЕТОДИ ПСИХОЛОГІЧНОГО ВПЛИВУ У КІБЕРЗЛОЧИННОСТІ

Сучасний цифровий простір став не лише каналом передачі інформації, але й полем інтенсивної психологічної експлуатації: кіберзлочинці дедалі частіше змушують жертв приймати рішення, що шкодять їх інтересам.

Актуальність теми випливає з росту кількості фішингових атак, компрометацій акаунтів та витоку персональних даних [3]. Сучасні кібератаки дедалі частіше використовують соціальну інженерію, маніпуляцію увагою та емоціями жертв для досягнення фінансової, інформаційної або ж репутаційної вигоди, що зумовлює високий ризик системних втрат, як на рівні окремих користувачів, так і організацій. Та незважаючи на прогрес у технічних засобах захисту, їхня ефективність значною мірою залежить від розуміння та протидії психологічним механізмам, що маніпулюють увагою, емоційним станом жертви та спираються на соціальні правила поведінки.

У загальному вигляді під *кіберзлочинами* міжнародна спільнота розуміє: незаконний доступ, нелегальне перехоплення, втручання у дані або систему, зловживання пристроями, пов’язані з комп’ютерами, підробки та шахрайство, всі види забезпечення обігу та використання дитячої порнографії за допомогою комп’ютерної мережі, а також порушення авторських прав. Їх особливість полягає в середовищі здійснення – кіберпросторі, де «віртуальні» об’єкти психологічно сприймаються як більш доступні та менш захищені. Значущим криміногенним фактором також є анонімність користувачів, що дозволяє приховати особу, тим самим вводячи в оману інших та виступати під чужим іменем.